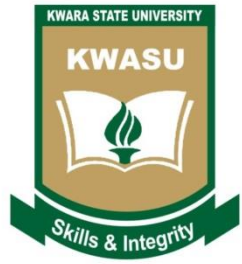
KWARA STATE UNIVERSITY



THE THIRD (3RD) INAUGURAL LECTURE

JUST FOR THE LOVE OF HIGH SPEED PROCESSORS

By

PROFESSOR KAZEEM ALAGBE GBOLAGADE
B.Sc. (Unilorin), M.Sc. (UI), Ph.D. (TuDelft, The Netherlands)
Head, Department of Computer Science
Provost, College of Information & Communication Technology
KWARA STATE UNIVERSITY, MALETE

5th March 2018

This Third (3rd) Inaugural Lecture was delivered under the Chairmanship of

The Vice Chancellor
Professor AbdulRasheed Na'Allah, PhD (Alberta)

5th March, 2018

ISBN: 978-978-54870-4-6

Published by
Kwara State University Press

Printed by: Unilorin Press



PROFESSOR KAZEEM ALAGBE GBOLAGADE

B.Sc. (Unilorin), M.Sc. (UI), Ph.D. (TuDelft, The Netherlands)

Professor of Computer Science

Courtesies

The Vice Chancellor,
The Deputy Vice Chancellor, Academics,
The Deputy Vice Chancellor, Administration,
The Registrar,
The Bursar,
The University Librarian,
Dean, School of Graduate Studies,
Provosts of Colleges,
Dean, Student Affairs and other Deans and Directors,
Professors and other Members of the Senate,
Heads of Departments and Units,
All other Academic Colleagues and non-Teaching Staff,
Government Officials,
My Lords Spiritual and Temporal,
Distinguished Students of the Department of Computer Science,
Gentlemen of the Press,
Distinguished Invited Guests,
Great KWASUITES,
Ladies and Gentlemen

1. Preamble

It is with a heart filled with gratitude and praise to the Almighty Allah, who has not only kept me alive but also given me the privilege to deliver the 3rd Inaugural Lecture of the Kwara State University.

Being a lecturer was not by accident. After the completion of my Advanced Level Course at the Kwara State Polytechnic, I applied to study Computer Science at the University of Ilorin – the now better by far University. I had wanted to study Mathematics but my father and my

brother, Professor Wasiu Alagbe Gbolagade did not permit me to opt for Mathematics. His simple reason was that Computer Science was more lucrative (at least as at that time) as he wanted me to be a better person. I give praises to God as I have no regrets following this path. I did my National Youth Service Corps (NYSC) at the University of Maiduguri in Borno State. Before I completed my National Service, there was a job opening for me at the Central Bank of Nigeria, which I did not take because I wanted to be a lecturer. Mr. Vice Chancellor, Sir, I started my academic career at the Olabisi Onabanjo University (OOU), Ago-Iwoye, Ogun State, Nigeria in January 2002 (more than sixteen years ago). In 2005, I left OOU shortly after my promotion to Lecturer II for University for Development Studies (UDS), Ghana as a Lecturer with enhanced step. In 2008, I became a Senior Lecturer and later on, I attained the Professorial status (Associate Professor) at UDS in Ghana. I thank the good destiny that led me to Ghana as I recorded a lot of unprecedented achievements at UDS in Ghana.

I was appointed FULL Professor in March, 2014 in this University and I thank the Vice Chancellor of this great citadel of learning, Professor AbdulRasheed Na'Allah and the entire Management for the opportunity given to me to reach the pinnacle of my chosen career.

2. Introduction

Mr. Vice Chancellor, Sir, permit me to make a few remarks before I proceed to the topic of today's inaugural lecture. The first remark is coming from Professor Temi Emmanuel Ologunorisa (Ologunorisa, 2011). It states that an inaugural lecture has three traditions as follows: an inaugural lecture is used to justify the appointment or promotion of the

concerned lecturer to the exalted status of a Professor; an inaugural lecture is used to solicit support for a discipline or a department to which the concerned lecturer belongs; and an inaugural lecture that is devoted to a systematic exposition of selected contemporary issues in which the concerned lecturer can shed some light. Mr. Vice Chancellor, Sir, can I say that today's inaugural lecture will fit in perfectly well with the first or third tradition having been appointed to Full Professorial position four years ago? I am just presenting my inaugural lecture, which I would have loved to present in 2014 immediately after my appointment as a Full Professor, but I am presenting it today due to institutional challenges far beyond my control. Mr. Vice Chancellor, Sir, the second remark is from Professor Lenrie Olatokunbo Aina, who, in his inaugural lecture of May, 2013 (Aina, 2013), categorised Professors into five, based on the length of time of their professorship as follows: (1.) Baby Professors, 0-4 years; (2.) Young Professors, 5-9 years; (3.) Adult Professors, 10-14 years; (4.) Old Professors, 15-19 years; and (5.) Aged Professors, 20 years and above. Mr. Vice Chancellor, Sir, I fall into the category of "Baby Professors" having been appointed a Full Professor in 2014 (4 years ago) and very soon, I will graduate from the class of "Baby Professors" to the class of "Young Professors". As a "Baby Professor", I believe presenting my inaugural lecture today is a great privilege and I thank the Vice Chancellor and the entire Management for this very rare opportunity.

Mr. Vice Chancellor, Sir, distinguished invited guests, ladies and gentlemen, I had a brief research sojourn in Numerical Computing and Computational Mathematics before destiny led me into Residue Number System, which

is a sub part of Computer Arithmetic, which is also a sub part of Digital Logic Design and which in turn is a sub part of Computer Architecture.

Today's inaugural lecture entitled: "Just for the Love of High Speed Processors", is the first coming from the College of Information & Communication Technology, of course the first coming from the Department of Computer Science and the third from Kwara State University. I chose this topic because of the significant efforts I have put in place in capacity building with regards to high speed processors and also because it encapsulates much of the thrust of my research in Computer Architecture.

3. What is a Processor?

A processor is the logic circuitry that responds to and processes the basic instructions that drive a computer. Also, a processor or "microprocessor" is a small chip that resides in computer and other electronic devices. Its basic job is to receive input and provide the appropriate output. While this may seem like a simple task, modern processors can handle trillions of calculations per second. The central processor of a computer is also known as the Central Processing Unit (CPU) ("Processor Definition," 2018).

Modern CPUs often include multiple processing cores, which work together to process instructions. While these "cores" are contained in one physical unit, they are actually individual processors. Processors that consist of two cores are called dual-core processors, while those with four cores are called quad-core processors. Some high-end workstations contain multiple CPUs with multiple cores, allowing a single machine to have eight, twelve, or even more processing cores ("Processor Definition," 2018).

A CPU has three components, namely: Arithmetic and Logic Unit (ALU), Memory Unit, and Control Unit.

Mr. Vice Chancellor, Sir, the focus of this lecture will be on CPU, specifically, the ALU. Like I said earlier, I was working on Numerical Computing and Computational Mathematics before destiny led me to Computer Architecture. As at that time, even though, I was interested in high speed computing, I did not know there was a strong relationship between Computer Arithmetic and Numerical Computing. The focus, on either Software Development or Computer Architecture, will tell which direction one should go.

4. Computer Architecture

Advances in Computer Architecture over the past two decades have allowed the performances of digital Computer hardware to continue its exponential growth, despite increasing technological difficulty in speed improvement at the circuit level. This phenomenon rate of growth, which is expected to continue in the near future, would not have been possible without theoretical insights, experimental researches, and tool-building efforts that have helped transform Computer Architecture from an art into one of the most quantitative branches of Computer Science and Engineering. In Computer designers' quest for user-friendliness, compactness, simplicity, high performance, low cost, and low power, Computer Arithmetic, plays a key role (Perhami, 2000). Computer Arithmetic, which is a subfield of Computer Architecture, is the focus of today's inaugural lecture. The major challenge in improving performance from the computational paradigm point of view is the reduction/elimination of the carry propagation

chains inherent in Weighted Number Systems (WNS), e.g., Binary Number Systems, and Decimal Number Systems. While this is an intrinsic performance limiter for arithmetic units and processors built based on WNS, several attempts have been made to overcome the speed limitations by following two main research avenues as follows: the carry propagation through the conventional ripple-carry adders, which is the main contributor to the addition delay and which can be accelerated by using fast addition techniques (Zimmermann, 1997). Those that make use of specialised circuitry are able to desterilise the carries calculation via methods like carry look ahead, carry-skip, prefix calculation, anticipated calculation, etc. These fast addition techniques are very important in improving arithmetic units performance because other arithmetic operations such as multiplication and division are based on addition, thus their delay heavily depends on the addition delay.

Mr. Vice Chancellor, Sir, an alternative way to speed up the addition process is to make use of number system with specialised carry characteristics, i.e., proposing alternative number representation systems, e.g., Redundant Signed Digit (RSD) number representation systems (Booth, 1951; Chen, 1985; Tocher, 1958; & Parhami, 1990) and Residue Number Systems (RNS) (Garner, 1959; Szabo & Tanaka, 1967; & Perhami, 2000). The sought characteristic of such alternative number systems is the capability to provide support for carry-free addition as this directly results to high-speed arithmetic units. The most important property of RSD number representation systems is the possibility of performing carry-free addition and borrow-free subtraction. Redundant number systems provide the possibility of addition with sub-logarithmic and even constant latency

(Jaberipur & Gorgin, 2010). Therefore, extremely fast constant-time addition can be performed with redundant number systems that support carry-free addition (Perhami, 2000). However, addition/subtraction in RSD requires limited carry since the carries are saved or stored and carry propagation delay occurs once at the very end of the computation (Perhami, 2000). Although algorithm for performing carry free addition is available, it is only valid if certain conditions are satisfied (Perhami, 2000). Thus, it is necessary to seek a number system, which generally supports carry free operations. The RNS (Garner, 1959; Szabo & Tanaka, 1967) is such an integer system exhibiting the capabilities to support parallel, carry-free addition, borrow-free subtraction, and digit by digit multiplication. Moreover, it provides support for fault tolerance (Szabo & Tanaka, 1967), which is becoming a crucial aspect as it is getting more and more expensive/difficult to fabricate perfect (predictable) devices in the context of deep sub-micron fabrication technologies. So far, most of the RNS related research has been done in the utilisation of RNS in Digital Signal Processing (DSP) applications, e.g., Digital Filtering, Convolutions, Correlations, Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Fast Fourier Transform (FFT). Similarly, RNS has been applied in low power design, number theory, digital communications.

Mr. Vice Chancellor, Sir, despite all these desirable RNS features, it has not been used widely in general purpose processors as the following RNS challenges must be properly addressed in order to be able to design RNS based general purpose architectures: sign detection, magnitude comparison, overflow detection, moduli

selection, residue to binary/decimal and vice-versa, division and other complex arithmetic operations. Effective data converters are required in order to efficiently implement the difficult RNS operations, e.g., magnitude comparison, sign detection, and division, and also to build fault tolerant RNS architectures. Thus, for general purpose RNS processors to become a reality, high-speed data converters are required. This is the major focus of today's inaugural lecture and I would like to seek the Vice Chancellor's indulgence to begin by giving some background information on the traditional reverse conversion methods, namely, the Mixed Radix Conversion (MRC) and the Chinese Remainder Theorem (CRT).

5. Traditional Reverse Conversion Methods

(a) Mixed Radix Conversion

For the moduli set $\{m_1, m_2, \dots, m_n\}$ with the dynamic range $\mathrm{M} = \prod_{\mathrm{i}=1}^{\mathrm{n}} m_i$, the residue number $\{x_1, x_2, \dots, x_n\}$ can be converted into the decimal number X, according to the MRC as follows (Gbolagade & Cotofana, 2009c):

$$X = \ell_1 + \ell_2 m_1 + \ell_3 m_1 m_2 + \cdots + \ell_n m_1 m_2 m_3 \dots m_{n-1} \quad (1)$$

where the Mixed Radix Digits (MRDs), $\ell_i, i = 1, n$ can be computed as follows (Wang et al. 2002), (Siewobr, Gbolagade & Cotofana, 2014):

$$\begin{aligned} \ell_1 &= x_1 \\ \ell_2 &= \left|(x_2 - \ell_1)\lambda_{1,2}\right|_{m_2} \\ \ell_3 &= \left|((x_3 - \ell_1)\lambda_{1,3} - \ell_2)\lambda_{2,3}\right|_{m_3} \\ \ell_n &= \left|(((x_n - \ell_1)\lambda_{1,n} - \ell_2)\lambda_{2,n} - \ell_{n-1})\lambda_{n-1,n}\right|_{m_n} \end{aligned} \quad (2)$$

where, $\lambda_{i,j}$ is the multiplicative inverse of m_i with respect

to m_j i.e. $\left|\lambda_{i,j} * m_i\right|_{m_j} = 1$.

Given the MRDs $a_i, 0 \leq \ell_i < m_i$, any positive number in the interval $[0, \prod_{i=1}^{n} m_i - 1]$ can be uniquely represented. The major MRC advantage as can be seen from Equation (2) the calculation of ℓ_i, i=1,n can be done only using arithmetic mod-m_i unlike CRT, which involves arithmetic mod-M, M being the system dynamic range, a rather large constant. The major drawback of the MRC is that by its very nature, it is a sequential process.

(b) Chinese Remainder Theorem

The traditional Chinese Remainder Theorem (CRT) is defined as follows. For a moduli set $\{m_1, m_2, \ldots, m_n\}$ with the dynamic range $\mathrm{M} = \prod_{i=1}^{n} m_i$, the residue number $\{x_1, x_2, \ldots, x_n\}$ can be converted into the decimal number X, according to the CRT as follows (Gbolagade & Cotofana, 2009a):

$$X = \left|\sum_{i=1}^{n} M_i |M_i^{-1} x_i|_{m_i}\right|_M \qquad (3)$$

where $M_i = \frac{M}{m_i}$ and M_i^{-1} is the multiplicative inverse of M_i with respect to m_i.

The main drawback of Equation (3) emerges from the required modulo-M operation which, given that M is a rather large number, this operation can be time consuming and rather expensive in terms of area and energy consumption.

The existing reverse converters are stemming from either the MRC or the CRT. Thus, all the discussions here follow the two techniques starting with MRC. The previously proposed fast MRC techniques either make use

of look up tables (Akkal & Siy, 2007, Huang, 1983, Jullien, 1978) or reduce the number of arithmetic operations that are involved in the conversion processes (Koc, 1991; Yassine & Moore, 1991; & Yassine, 1992). The later approach is desirable because a suitable reduction method can be utilised in conjunction with appropriate selection of moduli, which can produce unity for all the required multiplicative inverses in the conversion processes. This can lead to a fast and memory less reverse converter.

MRC based techniques, which considerably reduce the number of involved arithmetic operations during the conversion processes have been presented in (Yassine & Moore, 1991). It can be inferred from the description given in Equation 2 and in line with the discussion in (Yassine & Moore, 1991) that a total of $\frac{k(k-1)}{2}$ arithmetic subtractions and multiplications are required in order to compute the MRDs for k-moduli sets. This means that the conversion process that computes the MRDs for an RNS with k moduli set has an asymptotic complexity in the order of $O(k^2)$. The improved MRC described in (Yassine & Moore, 1991) requires a total of $\frac{k(k-1)}{2}$, 2 subtractions just as in Szabo & Tanaka, 1967 but can reduce the arithmetic multiplications to (k - 2) instead of $\frac{k(k-1)}{2}$, 2 required in (Yassine & Moore, 1991) for computing the MRDs. Even though the number of arithmetic multiplications was reduced, the asymptotic complexity was not improved beyond $O(k^2)$. We managed to resolve this issue and the resolution will be reported in this inaugural lecture.

As previously mentioned, the other research avenue followed by the RNS community is based on CRT. While for MRC, the discussion can be done in general, CRT based

converters have structures and performance which heavily depend on the moduli set they target. In view of that, our discussion in this inaugural lecture is organized per type/class of moduli. The large majority of available high-speed CRT based reverse converter architectures are based on the triple moduli set $\{2^n+1,2^n,2^n-1\}$ as they can exploit the useful properties of the numbers (2^n+1) or (2^n-1). However, the moduli sets {2n+1,2n,2n-1}and {2n+2,2n,2n-1} are also considered useful because the numbers are consecutive, enabling nearly equal width adders and multipliers in the hardware implementation (Wang, Song, Aboulhamid and Shen, 2002). Many of our contributions in this connection will be reported in this lecture.

6. Contributions to Knowledge

Mr. Vice Chancellor, Sir, permit me to enunciate my humble contributions to knowledge in the past sixteen (16) years. I have worked with a number of colleagues in the area of Moduli Selection, Reverse Conversion, Overflow detection and application of RNS, e.g., in Bioinformatics, cryptography, cloud computing, and wireless sensor networks.

7. Moduli Selection

(1) In Gbolagade (2009a), moduli selection in RNS, which is an important issue in the design of digital systems was investigated. Moduli Selection Guidelines (MSG) for the moduli sets {2n+2,n,2n-1}, {2n+1,2n,2n-1} and $\{2^n,2^n-1,2^{n-1}-1\}$ were proposed. A program based on the MSG for computing all possible multiplicative inverses that may be needed when using different conversion techniques was designed. Based on this experiment, it was deduced that

there is a well-established relationship between the form of the moduli set, the moduli and the multiplicative inverses. These deductions are used to come up with the moduli representations of the various multiplicative inverses. Hence, using the MSG, the cost of computing the multiplicative inverses is eliminated. The experimental results reveal that some of these multiplicative inverses will always be unity so their computations are no more needed. Consequently, the usage of these guidelines in building a RNS-to-decimal converter results in a considerable reduction in the number of arithmetic operations required during the conversion process. These results provide the possibility of a wide range of applications of RNS in Digital Signal Processing.

8. Mixed Radix Based Conversion Schemes

(2) We introduced RNS to MRC technique, which addresses the computation of Mixed Radix Digits in such a way that enables the MRC parallelisation. Given an RNS with a set of relatively prime integer moduli $\{m_1, m_2, \dots, m_n\}$, the key idea behind this proposed MRC technique is to maximise the utilisation of the modulo-m_i adders and multipliers present in the RNS processor functional units. For an n-digit RNS number X = $(x_1,x_2,x_3,\dots,x_n)$ this method requires k-iterations. However, at iteration i, the modulo-m_i units are utilised for the calculation of the MR digit a_i, while the other modulo units are calculating intermediate results required in further iterations. Given that one such iteration can be seen as one single operation in the RNS processor functional units, this approach results in an RNS to MR conversion with an asymptotic complexity, in terms of arithmetic operations, in

the order of O(k), while the traditional MRC and many other state of the art MRCs based techniques exhibit an asymptotic complexity in the order of $O(k^2)$. More particularly, the utilisation of our technique achieved 33.33% and 5.26% reductions with moduli sets of length four when compared with MRC and the improved MRC in (Yassine & Moore, 1991), respectively. For moduli sets of length ten, our proposal achieved 66.67% and 38.64% reductions when compared with MRC and the improved MRC in (Yassine & Moore, 1991), respectively. I presented this result at the IEEE International Symposium on Circuits and Systems (ISCAS 2009) in Taipei, Taiwan, China (Gbolagade & Cotofana, 2009c).

(3) We generalised a previously proposed technique that was restricted to 5-moduli set such that it can be utilised in conjunction with any RNS with the set of relatively prime integer moduli $\{m_1,m_2,m_3,\ldots,m_n\}$. Next, we simplified the computing procedure by maximising the utilisation of the modulo-m_i adders and multipliers present in the RNS processor functional units. For a n-digit RNS number $X = (x_1,x_2,x_3,\ldots,x_n)$, the proposed method takes at most n iterations. Each iteration, except the first one, requires two multiplications and one parallel subtraction over all the mod-m_i ways of the RNS adder. This scheme results in an RNS to MRC with an asymptotic complexity, in terms of arithmetic operations, in the order of O(n), while the traditional MRC technique exhibits an asymptotic complexity in the order of $O(n^2)$. In particular, the utilisation of our technique, for 3-moduli and 10-moduli RNS results in the reduction of the total number of arithmetic operations required by the conversion process with 40.00% and 77.16%, respectively, when compared to

the MRC in (Yassine, 1992). I presented this result at the IEEE Asia Pacific Conference on Circuits and Systems in Macao, China (Gbolagade & Cotofana, 2008a).

9. Moduli Set with Common Factors

(4) At this point, I would like to briefly report some of my humble contributions regarding moduli sets with common factors. Throughout the world, few researchers have contributed to this area. They are: A.B. Premkumar, W. Wang, M.N.S. Swamy, M.O. Ahmad, Y. Wang, K. A. Gbolagade, G.R. Voicu and S.D. Cotofana. In total, there are eight published papers available on this subject and six out of these articles were published by a Nigerian, the gentleman presenting his inaugural lecture and standing before all of you today. The six papers were published in Knoxville in USA (IEEE MWSCAS 2008) (Gbolagade & Cotofana, 2008e), California in USA (Gbolagade & Cotofana, 2008d), Netherlands (PRORISC 2008) (Gbolagade & Cotofana, 2008b), Spain (ACACES 2010) (Gbolagade, Voicu, & Cotofana, 2010a), Tunisia (ICECS 2009) (Gbolagade & Cotofana, 2009a) and Mexico (IEEE MWSCAS 2009) (Gbolagade & Cotofana, 2009b).

(a) In the first published article, we assumed a general moduli set m_i, i=1,3, where $m_1 > m_2 > m_3$, with the dynamic range $M_i = \frac{M}{m_i}$, a modified CRT that requires mod-m_3 instead of mod-M calculations was proposed. Subsequently, we further simplified the conversion process by focusing on {2n+2,2n+1,2n} moduli set, which has a common factor of 2. We introduced in a formal way a CRT based approach for this case, which requires the conversion of the {2n+2,2n+1,2n} moduli set into a moduli set with relatively

prime moduli, i.e., set $\left\{\frac{m_1}{2}, m_2, m_3\right\}$ when n is even, n ≥ 2 and $\left\{m_1, m_2, \frac{m_3}{2}\right\}$ when n is odd, n ≥ 3. We demonstrated that such a conversion can be easily done and does not require the computation of any multiplicative inverses. We further simplified the 3-moduli CRT for the specific case of {2n+2,2n+1,2n} moduli set. For this case the proposed CRT requires 4 additions, 4 multiplications, and all the operations are mod-m_3 in case n is even and mod-$\frac{m_3}{2}$ if n is odd. This outperforms state of the art converters in terms of the required operations. I presented this result at the 51st IEEE International Midwest Symposium on Circuits and Systems (MWSCAS 2008), Knoxville, USA (Gbolagade & Cotofana, 2008e).

(b) In the second, third, fourth, and fifth published papers on moduli set with a common factor, we proposed another new reverse converter for the moduli set {2n + 2,2n + 1, 2n} for any integer n > 0. We simplified the traditional CRT in order to obtain a reverse converter that uses mod-n instead of mod-(2n + 2)(2n) or mod-2n required by other state of the art equivalent converters. Next, we presented a low complexity implementation that does not require the explicit calculation of modulo operation in the conversion process as it is normally the case in the traditional CRT and other state of the art equivalent converters. In terms of area, our proposal requires four 2:1 adders and 2 multipliers while the best state of the art equivalent converter (Gbolagade & Cotofana, 2008d) requires one 3:1 adder, two 2:1 adders, and four multipliers. In terms of critical path delay, our scheme requires 3 additions and 1 multiplication with mod-n operations whereas the converter in (Gbolagade & Cotofana, 2008e) requires 2 additions and 2

multiplications with mod-2n operations. I presented this result at the 5th International Summer School on Advanced Computer Architecture and Compilation for Embedded Systems (ACACES 2010) Terrassa, Spain (Gbolagade, Voicu, & Cotofana, 2010a). This result, in terms of both area and delay, outperforms the one I presented at the 52nd IEEE International Midwest Symposium on Circuits and Systems (MWSCAS 2009), Cancun, Mexico (Gbolagade & Cotofana, 2009b).

(c) In the sixth published article on moduli set with a common factor, we proposed a general 4-moduli RNS conversion scheme and then presented a compact form of multiplicative inverses valid for both n odd or even for the moduli set $\{2n + 3, 2n + 2, 2n + 1, 2n\}$. This increases the dynamic range and the processing parallelism enabling efficient reverse conversion. The proposed CRT utilises the same or slightly larger area when compared to other existing techniques but all the operations are mod-m4. This outperforms state of the art CRTs in terms of the magnitude of the numbers involved in the calculation and due to this fact, our proposal results in less complex adders and multipliers. I presented this result at the 16th IEEE International Conference on Electronics, Circuits and Systems (ICECS 2009), Tunisia (Gbolagade & Cotofana, 2009c).

10. Linear Moduli Sets

(5) For the moduli set with common factors just discussed, the moduli sets must first be mapped to the moduli sets, which are relatively prime and apart from this transformation problem, the converters developed with the moduli set with common factors reduce the dynamic range

of the original moduli set by 1-bit. Due to these reasons, we will now demonstrate our efforts in exploring the possibilities of building efficient reverse converters using the moduli set {2n+1, 2n,2n-1}. Mr. Vice Chancellor, Sir, in this connection, we published two strong articles, which remain the hottest articles regarding {2n+1, 2n,2n-1} moduli set. Those articles were published in (a) XXIII Conference on Design of Circuits and Integrated Systems (DCIS 2008), Greenoble, France at the world trade centre where I was the only African scholar present (Gbolagade & Cotofana, 2008c). (b) The second article appeared at the IEEE Transactions on Very Large Scale Integration (VLSI) Systems in 2011 (Gbolagade, Voicu & Cotofana, 2011). This second article has gained me a lot of recognition within the Computer Arithmetic and RNS communities. I thank God for this.

We proposed a new reverse converter for the moduli set {2n+1,2n,2n-1}. First, we simplified the traditional CRT in order to obtain a reverse converter that utilises mod-(2n-1) operations instead of mod-(2n)(2n-1) and (2n + 1)(2n-1) operations required by the converters in Gbolagade and Cotofana, 2008c) & (Ahmad, Wang & Swamy, 1999), respectively. Next, we transformed the needed corrective addition of M into a corrective m_3 addition. We then presented a novel low complexity implementation that does not require the explicit use of modulo operation in the conversion process. The performance of the proposed converter is evaluated both theoretically, in terms of the required number of arithmetic operations and experimentally by Field Programmable Gate Array (FPGA) implementation. Theoretically speaking, the proposed converter requires one 3:1 adder, three 2:1 adders, and 2

multipliers while the one in Gbolagade and Cotofana, 2008c requires one 3:1 adder, two 2:1 adders, and four multipliers. In terms of delay the proposed scheme requires 3 or 4 additions and 1 multiplication whereas the converter in Gbolagade and Cotofana, 2008c requires 3 additions and 2 multiplications. Moreover, due to the fact that our scheme operates on smaller magnitude operands, it utilises less complex adders and multipliers, which potentially results in even faster and smaller implementations. For the experimental assessment, the converters were described in VHSIC Hardware Description Language (VHDL) and implemented on Xilinx Spartan 3 FPGA. We used a wide range of values of n for the implementation. The synthesis results indicate that, on average, the proposed converter is in terms of delay 14% and 15.8% faster with 27% and 21% area decrease, when compared to the reverse converters in Gbolagade and Cotofana, 2008c and Ahmad, Wang & Swamy, 1999, respectively. The proposed converter also consumes, on average, 18% and 8% less power when compared to the converters in Gbolagade and Cotofana, 2008c and Ahmad, Wang and Swamy, 1999, respectively.

11. Powers of Two Moduli Sets

(6) (a) Mr. Vice Chancellor, Sir, I will now turn to some of our contributions in building high speed converters using powers of two moduli sets. Powers of two moduli sets are very useful in building adder based reverse converters. They are also more applicable to Digital Signal Processing (DSP) applications requiring larger dynamic range when compared to the linear moduli set discussed earlier. We have made a number of significant contributions in this area. I wish to report at this point that several of our articles

appeared in IEEE and other related Conferences, book chapters and journals. I wish to report one of our articles that was published in 2010 in IEEE International Conference on Application Specific Systems, Architectures and Processors (ASAP 2010), Rennes, France (Gbolagade, Voicu, & Cotofana, 2010b). Mr. Vice Chancellor, Sir, I need to add that over five hundred papers were submitted to this conference while only thirty seven top rated articles were accepted for presentation and publication in which my article was part. This paper made Africa the highest in percentage ranking with respect to acceptance rate. That is, 100% acceptance coming from Africa as I was the only African scholar who submitted and got his paper accepted and published. For me, as an African scholar, finding myself in who is who in Science and Engineering, it was a great honour. The paper can be summarised as follows:

We proposed two new novel memory-less residue to binary converters for the moduli set $\{2^{n+1} - 1, 2^n, 2^n - 1\}$. First, we simplified the CRT to obtain a reverse converter that requires mod-$(2^{n+1} - 1)$ instead of both of mod-$(2^{n+1} - 1)$ and mod-$(2^n - 1)$ required by state of the art converter. Second, we further reduced the resulting architecture in order to obtain a reverse converter that utilises only Carry Save Adders (CSAs) and Carry Propagate Adders (CPAs). We reduced the large $(2^{n+1} - 1)(2^n - 1)$ adder to a simple adder with the consequence of a reduction in the dynamic range from M to M-$(2^n - 1)^2$. We demonstrated that the reduction penalty decreases exponentially as n increases and for values of $n \geq 5$, the reduction penalty is negligible ($\leq$ 0.0078%). We resolved the dynamic range limitation problem and proposed another converter, which is valid for the entire dynamic range. Theoretically speaking, the two

proposed converters are faster than the most effective equivalent state of the art converter, but one of them requires more hardware resources. Finally, we implemented our proposals and the most effective equivalent state of the art converter on a Xilinx Spartan 3 FPGA. The obtained results show that, on average and contrary to the theoretical results, our schemes significantly reduced the area cost with no delay penalty (Gbolagade, Voicu, & Cotofana, 2010b).

(b) We proposed two novel high speed memory-less residue to binary converters for the moduli set $\{2^{2n+1}- 1, 2^n, 2^n - 1\}$. First, we simplified the traditional CRT and obtained a new converter that only requires mod-$(2^{2n+1}- 1)$ operations. Further simplifications result in a very simple and efficient hardware structure, composed of only CSAs with End-Around Carries (EACs) and CPAs. We resolved the domain restriction problem and proposed another reverse converter, which is valid for the entire dynamic range. The theoretical analysis indicates that the two proposed reverse converters are faster than the one in Molahosseini, Navi, and Rafsanjani (2008)) in terms of delay, but one of them requires more hardware resources. We described the proposed reverse converters and the one in (Molahosseini, Navi, & Rafsanjani (2008)) in VHDL and carried out the implementation on an FPGA. We used a wide range of values of n for the implementation. The synthesis results indicate that, on the average, the proposed limited range CRT (proposal-I) and the proposed entire range CRT (proposal-II) respectively, are capable of performing the reverse conversion 13.40% and 13.20% faster, with extra costs of 3.29% and 22.75% in terms of area when compared with the one in (Molahosseini, Navi, & Rafsanjani (2008)). Additionally, the AT^2 efficiency

metric suggests that proposal-I and proposal-II are 24% and 3%, respectively, more efficient than the one in (Molahosseini, Navi, and Rafsanjani (2008)). These results appeared in the proceedings of IEEE International Symposium on Circuits and Systems (ISCAS 2010) in Paris, France (Gbolagade, Chaves, Sousa, & Cotofana, 2010). This result was generated when I was a visiting researcher at the Technical University of Lisbon (TULisbon) in Portugal (Gbolagade et al., 2010).

(c) We proposed three reverse converters for the new moduli set $\{2^{2n+1}- 1, 2^{2n}, 2^{n} - 1\}$. Two of the proposed reverse converters, namely CI and CIII are based on the traditional CRT while the third one, namely CII is based on the MRC. The CRT based reverse converters are better in terms of both area and delay, when compared to the MRC based reverse converter. Therefore, it can be inferred that the CRT is a better approach to design reverse converters for this class of moduli sets. The proposed reverse converters are memory-less and adder based and can be easily realised in VLSI circuits. We performed both theoretical and experimental evaluation of our proposal. The theoretical analysis shows the advantages of our scheme, which is supported by the experimental results. The obtained synthesis results suggest that, CI is able to improve the conversion computation time by about 6% while reducing the required hardware area by more than 3% when compared to CIII. On the other hand, CIII improves the conversion speed by about 17% and reduces the hardware resources by more than 4%, regarding the proposed CII reverse converter. The proposed CIII is about 11% faster and requires about 22% more hardware resources than the converter in (Molahosseini, Navi, &

Rafsanjani (2008)). Additionally, the AT^2 metric indicates that the proposed CIII is 5% better than the one in (Molahosseini, Navi, & Rafsanjani (2008)). (Gbolagade et al, 2010).

(d) For the use of the most popular traditional moduli set $\{2^n, 2^n\text{-}1, 2^n + 1\}$ in building effective reverse converters, we have made a number of significant contributions. First, we presented a modified CRT based reverse converter for the traditional moduli set $\{2^n, 2^n\text{-}1, 2^n + 1\}$. The proposed converter is memory-less and adder based. We performed both theoretical and FPGA experimentation of our scheme and that of the state of the art. From the theoretical assessment, we deduced that our converter is advantageous in terms of speed while requiring more hardware resources. Additionally, we implemented our scheme with the state of the art on Xilinx Spartan 6 FPGA. The results indicated that, on the average, and contrary to the theoretical result, our proposed reverse converter significantly outperforms the state of the art in terms of both speed and hardware resources. On the average, our proposed converter is 9.16% faster than the state of the art while in terms of hardware resources, our scheme saves about 24.05% hardware resources when compared with the celebrated converter presented by Wang, et al. (2002). This result was generated together with my former PhD student, Dr. Edem Bankas and published in the Journal of Computing (Bankas & Gbolagade, 2012). A simple lesson from this result to a novice can be in conformity with one of my propositions – "In principle, there should be no difference between theory and practice, but in reality there is".

(e) We hybridised the converter developed for the

moduli set $\{2^n, 2^n\text{-}1, 2^n + 1\}$ with the MRC in order to obtain an effective reverse converter for the moduli set $\{2^n, 2^n\text{-}1, 2^n + 1, 2^{2n+1}\text{-}1\}$. The proposed scheme is purely adder based and memory-less and was implemented in a two level design. The first level consists of deriving the equivalent weighted number of the residue (x_1,x_2,x_3) using the modified CRT algorithm for the popular moduli set $\{2^n, 2^n\text{-}1, 2^n + 1\}$ discussed earlier. Next, the resulting equivalent weighted number from the first level was hybridised with the fourth residue x_4 using the MRC with respect to the composite moduli set $\{2^{3n}\text{-}2^n, 2^{2n+1} - 1\}$. We further simplified the resulting architecture in order to obtain an adder based and memory-less reverse converter that utilises only CSAs and CPAs. We compared our scheme with the known existing state of the art proposed by Molahosseini, et al. (2010) both theoretically and experimentally. Theoretical assessment indicates that our proposal is better in terms of both area and delay than the state of the art. We implemented our scheme and that of the state of the art on FPGA. On the average, our scheme is 9.80% faster at the expense of 4.14% area loss. Area Time Square also indicated that our scheme is 19.34% better than the state of the art (Bankas & Gbolagade, 2013a).

(f) We proposed a new 5n bit DR moduli set $\{2^{2n}\text{-}1, 2^n, 2^{2n+1}\text{-}1\}$ derived from the four moduli set $\{2^n, 2^n\text{-}1, 2^n + 1, 2^{2n+1} - 1\}$ presented by Molahosseini et al. (2010) by combining $(2^n - 1)$ and $(2^n + 1)$ into $(2^{2n} - 1)$. Next, we proposed an efficient MRC based RNS-to-Binary converter for the new moduli set. When compared to the converter presented by Molahosseini et al. (2010), theoretically speaking, our converter outperforms the state of the art in terms of both hardware requirements and delay. FPGA

implementation results suggested that, averagely, our proposed scheme is 18.56% faster and saves about 17.36% hardware resources. This result was published in the International Journal of Circuits and Architecture Design (Bankas & Gbolagade, 2014a).

(g) We proposed an efficient RNS to binary converter for the moduli set $\{2^n, 2^{2n+1}-1, 2^{2n+2}-1\}$ which contains low-cost moduli. The proposed reverse converter is based on MRC. The resulting architecture has only one level of CSA. FPGA implementation results indicated that our proposed scheme outperforms the state of the art with approximately 35.98% and 6.76% in terms of area cost and conversion time, respectively. This result was published in the Computer journal (oxford) (Bankas & Gbolagade, 2014b).

(h) We proposed a new moduli set $\{2^{2n}, 2^{2n+1}-1, 2^{2n+2}-1\}$ which is an enhancement of the moduli set $\{2^n, 2^{2n+1}-1, 2^{2n+2}-1\}$ and its associated efficient RNS to binary converter. The proposed reverse converter is based on MRC. Divide and conquer approach was used to implement the MRC where the moduli set is grouped into two. The first phase combined the first and the second residue with respect to the subset $\{2^{2n}, 2^{2n+1}-1\}$. In the second phase, the result of the first phase is combined with the third residue with respect to the composite moduli set $\{(2^{2n})(2^{2n+1}-1), 2^{2n+1}-1,\}$. The synthesis results indicated that our scheme is capable of performing reverse conversion 32.75% faster and it is 49.21% cheaper regarding the known equivalent state of the art reverse converter. These results and similar other results we published on powers of two moduli sets can be found in Bankas and Gbolagade, 2013b; Bankas and Gbolagade, 2013c; Bankas, Gbolagade, and Cotofana, 2013; Gbolagade, 2011; Gbolagade, 2009b; Gbolagade,

2009c; Gbolagade, 2013.

12. Overflow Detection Schemes

(7) Mr. Vice Chancellor, Sir, I now wish to report some of our humble contributions in the area of Overflow Detection. I proposed several interesting overflow detection schemes with my former M.Sc students, late Mr. Hillary Siewobr, Mr. Peter Agbedemna and my former PhD student, Dr. Mohammed Ibrahim Daabo. Our contributions are summarised as follows:

Several efficient overflow detection schemes for RNS architecture were presented. The proposed techniques were based on residue comparison, group number, and Operand Examination Method (OEM). First, we proposed overflow detection schemes with residue to binary converters for the moduli sets $\{2^n-1,2^n,2^n+1\}$ and $\{2^{2n}-1,2^{2n},2^{2n}+1\}$. The proposed overflow detection schemes, which also perform reverse conversion using the remainder theorem, utilise the sum of operands by distributing the numbers in the system dynamic range into groups. Second, RNS overflow detection scheme, which utilises OEM was proposed for the moduli set $\{2^n-1,2^n,2^{2n+1}-1\}$. Third, OEM based overflow detection technique is also proposed for the moduli set $\{2^n-1,2^n,2^n+1,2^{2n}+1\}$ in order to enhance parallelism and to accommodate applications requiring larger dynamic range. Next, a generalised multiplicative overflow detection scheme using OEM for any length three moduli set was presented and for easy implementation of the proposed generalised scheme, the moduli set $\{2^n-1,2^n,2^{2n+1}-1\}$ was utilised. Again, based on residue comparison, we presented generalised multiplicative and additive overflow detection schemes for the moduli set {M-k, M}. The proposed

generalised schemes are applicable for moduli sets of any length. Theoretical analyses indicated that the proposed schemes require lesser hardware or faster (or both in some cases) when compared to the best known state of the art overflow detection schemes. These results and similar ones now reported here can be found in ((Daabo & Gbolagade, 2012a), (Daabo & Gbolagade, 2012b), (Daabo, Gbolagade, & Agbedemna, 2015), (Daabo, Gbolagade, & Agbedemna, 2016).

13. Applying RNS in Addressing Security Issues in Communications

(a) Modified Lempel-Ziv-Welch's (LZW) Algorithm

(8) Encryption and compression of data may be viewed as an aspect of information theory in which the primary objective is to minimise the amount of data to be stored or transmitted. Data compression entails the reduction of the amount of space needed to store or transmit data. In transmitting data through high-speed media, high-speed and secured data compression is desired. The LEMPEL-ZIV-WELCH'S (LZW) algorithm is one of the information compression algorithms that capitalises on the reoccurrence or repetition of words or phrases in a file for compression, reducing the number of bits or the execution time and security is therefore crucial in this research area. Due to RNS inherent features such as carry free, parallelism, and fault tolerant capabilities, it is considered suitable in operational time, area, and power reduction in data transmission process. Our contributions can be summarised as follows:

We proposed modified high-speed and secured data

compression algorithms. RNS has been efficiently applied to LZW data compression using different moduli sets ($\{2^n - 1,\ 2^n,\ 2^n + 1\}$ and $\{2^n - 1,\ 2^n,\ 2^n + 1,\ 2^{n+1} - 1\}$) which is an adaptation of LZW algorithm that codes strings of characters with codes of a fixed number of bits. A number of strategies or methods have been employed in the development of these new schemes. First, the LZW algorithm has been modified by applying RNS with the moduli set $\{2^n - 1,\ 2^n,\ 2^n + 1\}$, resulting in new efficient data encryption and decryption schemes (new encoder and decoder pairs which also allows for conversion from one number representation to the other). Second, the output of the LZW algorithm has been modified to allow for secrete bit stream or channel transmission of data through networks so that network intruders cannot make meaning of intercepted data. Third, despite the fault tolerance ability of RNS, error detection and correction mechanisms has been provided for by adding two extra moduli using Redundant Residue Number System (RRNS). This is because, most error detection and correction schemes in RNS employs the use of RRNS which involves the use of extra moduli. Fourth, the moduli set $\{2^n - 1,\ 2^n,\ 2^n + 1,\ 2^{n+1} - 1\}$, was also applied in the same fashion to investigate the effect of convertor type on the performance of the LZW compression algorithm. The moduli set was carefully chosen to work for only *n*, even (as agreed by both encoder and decoder pair) to enhance the security of the proposed scheme. Finally, simulations have been done using Matrix Laboratory (MatLab) for some documents (of varying sizes) a number of times and the averages taken for compression size and execution time to determine the efficiency of the proposed schemes which shows better performance than the

traditional LZW method. This proposed system has led to the development of new data encoding and decoding schemes as well as enhanced security, storage capacity, and speed of compression and transmission than the traditional LZW coding presented in the known equivalent state of the art compression and fault-tolerant schemes (Alhassan, Gbolagade & Bankas, 2015).

(b) **Modified Rivest Shamir Adleman (RSA) Algorithm**

(9) Sensitive information is transmitted across the internet every day and keeping such information as sacred is an important adventure. This is because malicious activities are on the increase as hackers are doing everything possible to steal such information. Rivest Shamir Adleman (RSA) encryption is the most widely used for securing sensitive information sent over an insecure channel like the internet. However, RSA has a difficult problem of encrypting smaller messages, m for which $m^e < n$, where e is the public component and n, the modulus.

We have presented several schemes for enhancing RSA encryption algorithms. First, an improved RSA cryptosystem based on Mixed Radix Conversion (MRC) was designed and implemented. This scheme utilises two stages of encryption. The first stage is the traditional RSA and the second stage is to further encrypt the cypher text obtained from RSA using smaller moduli. The first stage of the decryption process is to obtain a partial result through MRC. The final stage of decryption is the classical RSA decryption process. This is to enable a message m, for which $m^e < n$ to be encrypted. The obtained results indicated that the proposed system outperforms the existing

algorithm in terms of security when the message is to be encrypted. The private key length of the proposed scheme was found to be $10 - bit$ longer than the classical RSA encryption scheme. This indicates that the proposed scheme has the ability to withstand brute force attack than the classical RSA encryption scheme. Second, a new RSA encryption scheme based on the Chinese Remainder Theorem (CRT) with a high dynamic range was implemented. This is achieved by designing and implementing a scheme with two levels of encryption and a corresponding two level of decryption. The first level of encryption is the classical RSA encryption and in the second level of encryption, forward conversion technique was utilised. In the first level of decryption, the CRT was employed and the classical RSA decryption process was utilised for the second level of decryption. Encrypting messages $m \leq 20$ were found not to be secured using RSA scheme. However, encrypting same messages using the proposed scheme was found to be secured. The proposed scheme performs better than the state of the art in terms of propagation delay and cost. The propagation delay and cost of the state of the art are $(12n + 10)_{FA}$ and $(15n + 5)D_{FA}$ respectively, while the delay and cost of the proposed system are $(12n + 3)D_{FA}$ and $(16n - 2)D_{FA}$ respectively. Next, a new MRC based RSA with error detection and correction scheme is presented. Length-five moduli set is used where the first three are the information moduli and the last two are the redundant moduli. A forward converter was built using the information moduli set for purposes of data encryption in the second stage of encryption. MRC is employed to build a reverse converter using the information moduli set that will be used for the decryption process.

How the scheme detects and corrects an error was demonstrated. This scheme is found to detect and correct a maximum of $(2n+1)-bit$s errors occurring in the first modulus or the second modulus. This ensures a more reliable data communication using the proposed system than the RSA scheme. Additionally, a Residue Number System decoder pair was designed using a length-two moduli set for purposes of data compression and secured communication. This scheme was found to reduce the number of bits in a message to $40-46.15\%$ of its original size for larger messages and 14.29% for relatively smaller messages. This greatly decreases the traffic of the channel and hence increases the speed of transmission. This also reduces the transmission power needed to send data packets across the transmission channel (Salifu & Gbolagade, 2016a, Salifu & Gbolagade, 2016b, Salifu & Gbolagade, 2016c, Salifu & Gbolagade, 2017).

14. Conclusion and Recommendations

Mr. Vice Chancellor, Sir, I have presented a number of contributions that we have made towards RNS based processors realisation. I enumerated a number of challenges that preclude RNS usage in general purpose computing. Some of the challenges include: Moduli Selection, Overflow Detection, Sign Detection, Magnitude Comparison, Division and other Complex Arithmetic operations. While we have proffered sufficient solutions to some of the issues, some still require a lot of attention.

In the next couple of years, I will be busy investigating how other RNS Challenges not covered in this presentation, will be solved.

In my more than sixteen years' experience as a

University teacher and administrator, I wish to make the following recommendations, which I believe will further improve University education in this country.

(a) For Higher Education Institutions

(i) Expanding support for scholarship and introducing rigorous performance expectations. Apart from the institutional TETFUND support, Universities should try to create a special FUND to assist identified exceptional scholars not able to attract international/national research grants. There should be a very rigorous performance expectation guidelines set up for the winners of such grants.

(ii) Strengthening the system of mentoring in order to facilitate research proposal writing and publication skills. This, I believe will have overall advantage on the University System.

(iii) In a University System, teaching component should be made an integral part of the requirements for the award of a PhD degree.

(iv) Universities must engage with international development partners in order to explore international funding opportunities. These grants may be utilised by our PhD supervisors to attract bright PhD students from within and outside Nigeria.

(v) The mode of teaching of GNS computer science courses should be revised. Computer Laboratories must be made available for teaching these courses as it must be hands on practical training. With these, the number of educated illiterates will reduce significantly.

(vi) The Computer Science curriculum requires a review especially with respect to the number of programming languages computer scientists need to learn.

One suggestion is that the number of programming language courses can be narrowed down to either one or two. For example if an object oriented programming language such as Java (Java I) is taught in first semester of year 2, then Java II should be taught in the Rain Semester of year 2. Consequently, Data Structures, Design and Analysis of Algorithms, Software Engineering, Compiler Construction, Computer Graphics, etc., will be implemented in JAVA. With these, I believe computer science graduates will be well grounded.

(b) For Government

(i) Government should embark on massive sensitisation programmes such that wealthy citizens and especially the University alumni will come to the aid of our Universities through endowment, scholarships, loans, gifts, and donations as it is the case in the developed countries.

(ii) In order for our country to achieve the desired change, University Scholars should be involved in key decision making and place them in strategic positions.

(iii) More reliable and affordable IT infrastructures should be provided.

(iv) Special Funds should be created to assist IT start-up businesses.

(v) IT industries should be developed through research centres in order to facilitate strong collaboration between researchers and industries.

Acknowledgements

Mr. Vice Chancellor, Sir, at this point, I need to pay some tributes. This section is the most challenging aspect of this lecture as it is almost impossible to acknowledge everyone

who had played significant roles in one's life. Thus, I seek for forgiveness for any omission.

First of all, I thank God Almighty for making today a reality. I affirm that there is no god except ALLAH (SWT), who has no partner nor equal and who does as He wishes, the owner of the Heavens and the Earth and who created us from nothing to something and one who will return us to nothing again and then back to something. I am very grateful to ALLAH for taking me to the pinnacle of my chosen career.

Next, I appreciate all of you for honouring me today but I wish to mention some people for the roles they played in my career and life.

I would like to thank my late parents, Alhaji Isiaka Alagbe Gbolagade and Alhaja Khafilat Ayoni Gbolagade for their efforts in raising me up. Words alone cannot express my gratitude to both of you. May ALLAH grant the two of you Aljanat Fridaous.

I thank the Vice Chancellor of this great University, Prof. Abdul-Rasheed Na'Allah, for the roles he has played in my academic growth and development.

I thank the two Deputy Vice Chancellors: Professor Suleiman Jamiu and Professor Saka Mahmud.

I appreciate our well experienced Registrar, Mr. Surajudeen Oyebode, the University Bursar, Alhaji Mohammed Ndache and the University Librarian, Mallam Atunde Alao for their love and support always.

I thank my fellow Provosts, Deans and Directors for the harmonious working relationship.

I sincerely thank KWASU Inaugural Lecture's committee: Professor Bayo Lawal (Chairman), Prof. Solihu Kabir, Mr. Michael Dada for the roles they have played to

make this inaugural lecture a successful one.

I thank all the members of staff of the College of ICT.

I thank Dr. M.O. Ibeun (HOD, LIS), Prof Tanure Ojaide (former), Dr. Isiaka Aliagan (present), HOD, Mass Comm, and my College Officer, Mr. Kayode Ajibade.

I am grateful to all the members of staff of the Department of Computer Science: Dr. R.M. Isiaka, Dr. (Mrs) R.S. Babatunde, Dr. (Mrs) J.F. Ajao, Mr. S.O. Abdulsalam, Mr. A.N. Babatunde, Mrs B, F. Balogun, Mrs. R. S. Suleiman, Mr. Peter Oyinloye, Mr Olatunji M. Abdulkadir, Mr. Babatunde Usman, and Mr. Damilola Popoola.

I thank my undergraduate's lecturers for laying a very strong foundation (at the University of Ilorin): Prof. J.A. Gbadeyan, late Prof. E.A. Bangudu, Prof. T.O. Opoola, Prof. J.S. Sadiku, Prof. O.M. Bamigbola, Prof. T.S. Ibiyemi, Prof. O.A. Taiwo, Prof. R.B. Adeniyi (my supervisor), Prof. O.O. Olugbara, Prof. E.A. Adebiyi and others. May God mightily bless you all.

I appreciate the contributions of my M.Sc lecturers (at the University of Ibadan): Prof. (Mrs). A.O. Osofisan, Prof. Bamidele Oluwade, Dr. Akinkunmi, Dr. Adeyemo, Dr. Osunade, Dr. C.R. Nwozo (my supervisor) and others. May God continue to shower His infinite mercies and blessings on you all.

I cannot thank my PhD supervisors (at the Delft University of Technology, The Netherlands) enough for exposing me to carrying out quality research: Particularly, I thank Prof. Sorin Dan Cotofana (advisor/co-promotor), Prof. H.J. Sips (promotor), Prof. Koen Bertels, Prof. Said Hamdiou and others. May God continue to bless you.

I thank my collaborators: Prof. L. Sousa (TU Lisbon,

Portugal), Dr. R. Chaves (TU Lisbon, Portugal), and Dr. G.R. Voicu (TU Delft, The Netherlands).

Specifically, I would like to thank all my past and present undergraduate and postgraduate students at Kwara State University, University for Development Studies, Ghana, Olabisi Onabanjo University, Federal University of Technology, Minna, Sule Lamido University, Jigawa, and Kano State University of Science & Technology, Kano, most especially Dr. A.Y. Omari-Sasus, Dr. E.K. Bankas, Dr. M. Daabo, Dr. M. M. Iddrisu, Dr. A. Alhassan, Dr. A. Salifu who has just bagged his Ph.D in KWASU and my numerous M.Sc students, for making teaching interesting and enjoyable.

I thank all members of staff of Olabisi Onabanjo University (OOU), Ago-Iwoye, Ogun State: Prof. Afolabi Soyode, (Former Vice-Chancelor, OOU), Prof. S. Bankole, (Former Dean, Faculty of Science, OOU), Late Prof Afolabi Adebanjo (Former Dean, Faculty of Science OOU), Prof. Ogunsanwo, (Former Dean, Faculty of Science OOU), Prof Chukwuma, (Former Head, Department of Physics, OOU) and Prof. Kola Odunaike (Dean, Faculty of Science OOU), Dr. M.A. Usman, (former Head, Department of Mathematical Sciences, OOU), Drs. Ogunwobi, O.B. Oyatokun, Olatayo, Agunbiade, A.U. Rufai, Tunji Abiala, Solanke, Hammed, Odetunde, Efuwape, M.O. Olayiwola and other teaching and non-teaching staff members of Department of Mathematical Sciences. I thank you all for your sterling contributions.

I thank all the members of staff of the University for Development (UDS), Ghana: Late Prof. Kaburise (Former VC, UDS), Prof. K.S. Nokoe (Former Ag. VC, UDS), Prof. Haruna Yakubu (Former VC, UDS), Prof. Gabriel Teye

(VC, UDS), Prof. David Millar (Former PRO VC, UDS), Prof. Seidu Alhassan (PRO VC, UDS), Late Prof K. Aboagye (Formal Dean, SMHS), Prof. Bacho (Former Dean-in Charge, Wa Campus), Prof. Ameen Alhassan, Prof. Daniel Bagah, Prof. Sylvester Gala, Prof. Kpeligba (Former Dean-in Charge, Navrongo Campus), Prof. Luguterah (Dean, FMS), Prof. Seini, Dr. ABT Zakaria (Registrar, UDS), Alh. Antwi (Ag. Librarian, UDS), Alh. Mohammed Hardi (Finance Officer, UDS).

I thank the following academic and Professional friends: Prof. (Engr) Mohammed Gana Yisa – Nigeria Ambassador to Japan, Prof. Temidayo Oladiji, Prof. M.O. Ibrahim, Dr. R.G. Jimoh (Associate Prof.) - UNILORIN, Prof. O.S. Olabiyisi and Prof. E. Omidiora - LAUTECH, Prof. M. Aminu (UDU, Sokoto), Prof. Taura, Dr. Kabir and Mr. Olayiwola - SLU, Jigawa, Drs. Mikail, Kolo, and Engr Ajao - FUTMINNA, Dr. Abubakar (Deputy VC, KUST, Wudil), Mr. Yazid-KUST, Prof. O. Awodele and Prof. Y. Adekunle - Babcock University, Ilishan-Remo, Ogun State, Prof. G.A. Aderounmu (President, NCS), Prof. C.O. Uwadia, Prof. C. Akinyokun, Prof. A.S. Sodiya, and Prof. C.K. Ayo (Former VC, Covenant University).

Special thanks go to my brother and mentor, Professor Wasiu Alagbe Gbolagade, for automatically taking over the fatherly roles. Just mere words of thanks can never be enough to describe your support and assistance. May God in His infinite mercies reward you abundantly. I appreciate the members of our family: Mr. Asimi Adeniyi, Alhaji Ismaila Alagbe, Mr. Rauf Fatai, Mr. Rauf Makaila, Alhaji Buli Adegboyega, Mr. Semiu Alagbe (Kosewu), Mr. Haruna Adekunle Adeniyi, Mr. Ismaila Lanre Ajao, Mr. Yisau Akanji Saliu, alhaja Silifat Alagbe, alhaja Afusat

Asake Popoola, alhaja Saidat Anike Badrudeen, Mrs Ramotalahi Gbolagade, Mrs Biodun Gbolagade, Mrs Alimat Alagbe, Mrs Adegboyegas, Mrs. Rauf, Miss Marufat Adedamola Gbolagade, Badrudeen Mariam, AbdulJeleel Popoola. I acknowledge all the Alagbes and Gbolagades.

I thank my in-laws, Alhaji and Alhaja Mudasiru for giving me a beautiful and responsible daughter. May Allah grant you long life. Mr. Fatai Mudasiru is also highly acknowledged.

I would also like to thank all my childhood friends and Professor Kazeem Gbolagade's inaugural committee from Iwo: Gbadegesin Asimiyu, Engr. Sarafadeen Soladoye, Alhaji Alidu Akibu, Dr. O.O. Olaewe, Surveyor Ayinde Rasaq, Mr. Oyebamiji Musiliu, Mr. Lekan Imran, Mr. Adelasoye Bolaji, Mr. Lukman Owotutu, Mr. Mutalubi Olawale, and Engr. Biodun Badrudeen, Otunba Kamaldeen.

I wish to acknowledge Professors Aderemi Abubakare, Layi Olurode, O. Oladipupo, Akanji Nasir, M.O. Fawole, Ayinde, and O.J. Alamu.

I specially thank all the members of our royal families in Iwo. I wish to thank our royal fathers, the Kabiesis and Chiefs, here present. I thank you for honouring me with your presence. *"Ki ade pe lori, ki bata pe lese, igba odun, odun kan".* Amin.

I wish to thank our Imams and Alfas for your constant and continuous prayers. May Allah continue to answer your prayers.

I thank my lovely children - Kazeem Gbolagade, Khadijat Gbolagade, Kamorudeen Gbolagade, Khafilat Gbolagade and Kabirat Gbolagade for being sources of joy to me always.

Lastly but certainly not the least, I thank my dear wife, Mrs Balqees Abidemi Gbolagade for all she has been doing for me since 1995. She is a friend of over two decades. She stood by me through thick and thin, and she is the only person in the world that understands me better. You have been pillars of support to me and my children. I thank you for doing a good work in my professional fulfilment and for nursing KAZYBAL International Schools to greater heights and through her I thank all the members of staff of KAZYBAL.

Mr. Vice Chancellor, Sir, distinguished invited guests, ladies and gentlemen; I thank you all for your presence, patience and attention. May God Almighty bless you all.

References

Ahmad, M. O., Wang, Y. & Swamy, M.N.S. (1999). Residue to Binary Number Converters for three moduli sets. *IEEE Trans. on Circuits and Systems-II, 46*(7), 180-183.

Aina, L. O. (2013). *Information, knowledge and the gatekeeper* (132nd Inaugural Lecture). Ilorin: University of Ilorin.

Akkal, M., & Siy, P. (2007). A new mixed radix conversion algorithm MRC II. *Journal of Systems Architecture, 53*, 577-586.

Alhassan, A., Gbolagade**,** K. A., & Bankas, E. K. (2015). A novel and efficient LZW-RNS scheme for enhanced information compression and security. *International Journal of Advanced Research in Computer Engineering and Technology (IJARCET), 4*(11), 4015-4019.

Bankas, E. K., & Gbolagade**,** K. A. (2012). A speed efficient RNS to binary converter for the moduli set $\{2^n, 2^n-1, 2^n+1\}$. *Journal of Computing 4*(5), 83-88.

Bankas E. K., & Gbolagade**,** K. A. (2013a). A residue to binary converter for a balanced moduli set $\{2^{2n+1}-1, 2^{2n}, 2^{2n}-1\}$. 5th International Conference on Awareness Science and

Technology (ICAST 2013), pp. 212-216, Aizu-Wakamatsu, Japan, 2–4 November.

Bankas, E. K., & Gbolagade**,** K. A. (2013b). A new efficient FPGA design of residue-to-binary converter. *International Journal of VLSI Design and Communication Systems (VLSICS), 4*(6), 1–11.

Bankas, E. K., & Gbolagade**,** K. A. (2013c). A new efficient RNS reverse converter for the 4-moduli set $\{2^n, 2^n-1, 2^n+1, 2^{2n+1}-1\}$. *International Journal of Computer and System Sciences. World Academy of Science, Engineering and Technology (WASET), 8*(2), 1-5.

Bankas, E. K., & Gbolagade**,** K. A. (2014a). An efficient VLSI design of a new CRT based reverse converter for the moduli set $\{2^n, 2^{2n}-1, 2^{2n+1}-1\}$. *International Journal of Circuits and Architecture Design, 1*(3), 211 – 221.

Bankas, E. K., & Gbolagade**,** K. A. (2014b). A new MRC adder-based reverse converter for the moduli set $\{2^n, 2^{2n+1}-1, 2^{2n-2}-1\}$. *The Computer journal*, *12*, 1-7.

Bankas, E. K., Gbolagade**,** K. A., & Cotofana, S. D. (2013). An efficient CRT based reverse converter for a novel moduli set $\{2^{2n+1}-1, 2^{2n+1}, 2^{2n}-1\}$. 24th IEEE International Conference on Application-Specific Systems Architecture and Processors (ASAP 2013), pp. 142-146, Washington DC, USA, 5–7 June.

Booth, A. D. (1951). A signed binary multiplication technique. *Quarterly Journal of Applied Maths*, *4*(2), 236-240.

Chen, T. C. (1985). Maximum redundancy signed-digit systems. Proceedings of IEEE Symposium on Computer Arithmetic, pp. 296-300. Urbana.

Daabo, M. I., & Gbolagade**,** K. A. (2012a). Overflow detection in RNS multiplication before forward conversion. *Journal of Computing, 4*(12), pp. 13-16.

Daabo, M. I., & Gbolagade**,** K. A. (2012b). RNS overflow detection scheme for the moduli set {M,M-1}. *Journal of Computing*, *4*(8), 39-44.

Daabo, M. I., & Gbolagade**,** K. A., & Agbedemna, P. A. (2015).

A combined scheme for overflow and reverse conversion for the moduli set $\{2^{2n}-1,2^{2n},2^{2n}+1\}$. *Transactions of the Nigerian Association of Mathematical Physics, 1*, 127-132.

Daabo, M. I., & Gbolagade**,** K. A. and Agbedemna, P. A. (2016). Fast overflow detection scheme by operand examination method for length three moduli sets. *Computer Engineering and Intelligent System, 7*, 8-13.

Garner, H. L. (1959). The residue number system. *IRE Transactions on Electronic Computers, EC-8*(2), 140-147.

Gbolagade**,** K. A. (2009a). Moduli selection guidelines for efficient residue-to-decimal conversion. *Far East Journal of Electronics and Communications, 3*(1), pp. 53-67.

Gbolagade**,** K. A. (2009b). A memoryless MRC technique for RNS-to-binary conversion using the moduli set $\{2^{n},2^{n}-1,2^{n-1}-1\}$. *International Journal of Soft Computing, 4*(3), 127-130.

Gbolagade**,** K. A. (2009c). A shorter algorithm for efficient residue to decimal conversion. *Advances in Computer Science and Engineering, 3*(2), pp. 147-156.

Gbolagade**,** K. A. (2011). New adder-based RNS-to-binary converters for the $\{2^{n-1}+1,2^{n-1}-1,2^{n}\}$ moduli set. *ISRN Signal Processing Journal, 7*, 1-7.

Gbolagade**,** K. A. (2013). An efficient MRC based RNS-to-binary converter for the $\{2^{2n}-1,2^{n},2^{2n+1}-1\}$ moduli set. *International Journal of Advanced Research in Computer Engineering & Technology, 2*(10), 2661–2664.

Gbolagade**,** K. A., Chaves, R., Sousa, L., & Cotofana, S. D. (2010). An improved RNS reverse converter for the $\{2^{2n+1}-1,2^{n},2^{n}-1\}$ moduli set. IEEE International Conference on Circuits and Systems (ISCAS 2010), pp. 2103-2106, Paris, France.

Gbolagade**,** K. A., & Cotofana, S.D. (2008a). Generalized matrix method for efficient residue to decimal conversion. Proceedings of 10^{th} IEEE Asia Pacific Conference on Circuits and Systems, pp. 1414-1417, Macao, China, December.

Gbolagade**,** K. A., & Cotofana, S. D. (2008b). MRC technique for RNS to decimal conversion for the moduli set {2n+2,2n+1,2n}. Proceedings of 16th Annual Workshop on Circuits, Systems, and Signal processing, pp. 318-321, Veldhoven, The Netherlands, 27-28 November.

Gbolagade**,** K. A., & Cotofana, S. D. (2008c). An efficient RNS to binary converter using the moduli set {2n+1,2n,2n-1}. XXIII Conference on Design of Circuits and Integrated Systems (DCIS 2008), Greenoble, France, 12-14 November.

Gbolagade**,** K. A. & Cotofana, S.D. (2008d). A residue to binary converter for the {2n+2,2n+1,2n} moduli set. Asilomar Conference on Signals, Systems, and Computers, pp. 1785-1789, California, USA, 26-29 October.

Gbolagade**,** K. A. & Cotofana, S.D. (2008e). Residue Number System Operands to Decimal Conversion for 3-Moduli Sets, Proceedings of 51st IEEE International Midwest Symposium on Circuits and Systems, (MWSCAS 2008), pp. 791-794, Knoxville, U.S.A., 10-13 August.

Gbolagade**,** K. A., & Cotofana, S. D. (2009a). A reverse converter for the new 4-moduli set {2n+3,2n+2,2n+1,2n}, 16th IEEE Int. Conference on Electronics, Circuits and Systems, (ICECS 2009), pp. 113-116, Tunisia, 13–16 December.

Gbolagade**,** K. A. & Cotofana, S. D. (2009b). Residue-to-Decimal Converters for Moduli Sets with Common Factors, Proceedings of 52nd IEEE International Midwest Symposium on Circuits and Systems, (MWSCAS 2009), pp. 624-627, Cancun, Mexico, 2-5 August.

Gbolagade**,** K. A., & Cotofana, S. D. (2009c). An O(n) residue number system to mixed radix technique. Proceedings of IEEE International Symposium on Circuits and Systems (ISCAS 2009), pp. 521-524, Taipei, Taiwan, 24-27 May.

Gbolagade**,** K. A., Voicu, G. R. & Cotofana, S.D. (2010a). An efficient FPGA design of reverse converter for the moduli set {2n+2,2n+1,2n}. 5th International Summer School on

Advanced Computer Architecture and Compilation for Embedded Systems (ACACES 2010), pp. 117-120, Terrassa, Spain, 11-17 July,

Gbolagade**,** K. A., Voicu, G. R., & Cotofana, S. D. (2010b). Memoryless RNS-to-binary converters for the $\{2^{n+1}-1,2^n,2^n-1\}$ moduli set. 21st IEEE International Conference on Application-Specific Systems Architecture and Processors (ASAP 2010), pp. 301-304, Rennes, France, 7-9 July.

Gbolagade**,** K. A., Voicu, G. R., & Cotofana, S. D. (2011). An efficient FPGA design of residue-to-decimal converter for the moduli set {2n+1,2n,2n-1}. *IEEE Very Large Scale Integration (VLSI) journal*, *19*(8), 1500-1503.

Huang, C.H. (1983). A fully parallel mixed-radix conversion algorithm for residue number applications. *IEEE Transactions on Computers, C32*, 398-402.

Jaberipur, G., & Gorgin, S. (2010). An improved maximally redundant signed digit adder. *Journal of Computers and Electrical Engineering, 36*, 491-502.

Jullien, G. A. (1978). Residue number scaling and other operations using ROM arrays. *IEEE Transactions on Computers, C27*, 325-336.

Koc, C. K. (1991). An improved algorithm for mixed radix conversion of residue numbers. *Journal of Comp Math App*., *22*(8), 63-71.

Molahosseini, A.S., Navi, K., & Rafsanjani, M.K. (2008). A new residue to binary converter based on mixed-radix conversion. 3rd International Conference on Information and Communication Technologies: from Theory to Application (ICTTA 2008), pp. 1-6, April.

Ologunorisa, T.E. (2011). *In search of climate justice and equity* (Inaugural Lecture Series 001). Osogbo, Nigerian: Osun State University.

Parhami, B. (1990). Generalized signed-digit number system: A unifying frame-work for redundant number representation. *IEEE Transactions on Computers*, *39*(1), 89-98.

Parhami, B. (2000). *Computer arithmetic: Algorithms and hardware design*. New York, Oxford University Press.

Processor Definition. (2018). Retrieved 19-01-2018 from https://techterms.com/definition/processor

Salifu A., & Gbolagade**,** K. A. (2016a). Mixed radix conversion based rsa encryption system. *International Journal of Computer Application (IJCA), 150*, 43-47.

Salifu A., & Gbolagade**,** K. A. (2016b). An improved redundant residue number system based error detection and correction scheme for the moduli set $\{2^{2n+1}, 2^{n+1}+1, 2^{n+1}-1, 2^n+1, 2^n\}$. *Advances in Wireless Communications and Networks, 2*(1), 11-14.

Salifu A., & Gbolagade**,** K. A. (2016c). A new RSA encryption scheme with error detection and correction. *The Journal of Computer Science and Its Applications*, *23*(2), 30-38.

Salifu A., & Gbolagade**,** K. A. (2017). An improved residue number system based RSA cryptosystem. *International Journal of Emerging Technologies in Computational and Applied Sciences*, *20*(1), 70-74.

Siewobr H., Gbolagade**,** K. A., & Cotofana, S. D. (2014). An efficient residue-to-binary converter for the new moduli set $\{2^{n/2}\pm1, 2^{2n+1}, 2^n+1\}$. International Symposium on Integrated Circuits (ISIC 2014), pp. 215-219, Singapore, 10–12 December.

Szabo, N., & Tanaka, R. (1967). *Residue arithmetic and its application to computer technology*. New York: MC-Graw-Hill.

Tocher, K .D. (1958). Technique for multiplication and division for automatic binary computers. *Quarterly Journal of Applied Maths*, *11*(3), 364-384.

Wang, Y., Song, X., Aboulhamid, M. & Shen, H. (2002). Adder based residue to binary number converters for $\{2^n+1, 2^n, 2^n-1\}$. *IEEE Trans. on Signal Processing, 50*, 1772-1779.

Yassine, H. M. (1992). Matrix mixed-radix conversion for RNS arithmetic architectures. 34th Midwest Symposium on

Circuits and Systems, pp. 273-278.
Yassine, H. M., & Moore, W. R. (1991). Improved mixed-radix conversion for residue number architectures. IEEE ISCAS Proceedings, pp. 191-200.
Zimmermann, R. (1997). *Binary adder architectures for cell based VLSI and their synthesis* (PhD Dissertation), Federal Institute of Technology, Swiss.