International Journal of Research in Engineering, Science and Management
Volume-3, Issue-2, February-2020
www.ijresm.com | ISSN (Online): 2581-5792

FPGA Implementation of Chinese Remainder Theorem Over Residue Modulo

Hanu Skanda Banappa[1], S. Hemanth[2], S. Vignesh[3], Chathrapathi Shivaji[4], G. Vasudeva[5]

[1,2,3,4]*Student, Dept. Electronics and Communication Engineering, Atria Institute of Technology, Bangalore, India*

[5]*Professor, Dept. Electronics and Communication Engineering, Atria Institute of Technology, Bangalore, India*

***Abstract*: Cryptography is a vast field that studies the methods of protecting information and communication through the use of techniques derived from mathematical concepts and sets of rule-based calculations called algorithms to transform messages in a way that are hard to decipher. The prefix “Crypt” means “hidden” or “vault” and the suffix “graphy” means “writing”. In the mathematics of integers, a modular concept is of prior importance in the cryptography community. It is a system that helps the number of integers (positive integers) to “wrap-around” when it's reaching a certain value - The Modulus (in plural moduli). Modular arithmetic can be taken care of mathematically by using integers that are compatible with the operations such as Addition, Subtraction and Multiplication. Residue modulo is a process of obtaining the proper remainder of any two integers resulting from a division process. Using the residue modulo technique in the chinese remainder theorem we can obtain GCD’s (greatest common divisor) of any 2 co-prime numbers. The chinese remainder theorem is used to integrate large numbers of integers as it is easier to compute with reduces the number of steps. Using the chinese remainder theorem we are implementing the “Winogard’s small convolution algorithm”. At the end of this we are intended to implement short-length DFT’s.**

***Keywords*: Cryptography, Algorithms, Modulus, GCD, Chinese remainder theorem, Winograd.**

1. Introduction

Cryptography is the study of securing the data present from a third party by creating written or generated codes. Cryptography converts the data into an unreadable format, allowing the data to be transmitted without it being decoded by an unknown entity, thus compromising the data. Cryptography is used in information security in many levels. The information cannot be decrypted and retrieved without a key. The information is made to maintain its integrity while being transmitted and(or) stored. Cryptography also aids in nonrepudiation, meaning that the sender and the delivery of a message can be verified. There are many ways of writing algorithms to encode data, some of the algorithms include-

- Secret key cryptography(SKC): IN this type of algorithm there exists only one key for both encryption and decryption.
- Public key cryptography(PKC): IN this type of algorithm 2 keys are used. This type of encryption is called Asymmetric encryption. One key is public and anyone can access it, the other key is a private key which can be accessed only by a private user. Sender encrypts the information using the public key and the receiver decrypt the data by using the private key.
- Hash Function: These types of algorithms are different from SKC and PKC. They do not use any key(also called one-way
  Encryption)for either encryption or decryption process. Hash function is mainly used to ensure that the file remains unchanged.

Modern day Cryptography concerns itself with the following objectives,

- Confidentiality: The information should be kept safe from any third party/ unauthorised personnel accessing it.
- Integrity: the information should be kept safe from any unauthorized entity to alter the content of the data storage or during the transfer of data from sender to receiver.
- Non-repudiation: The sender of the information/data cannot deny in later stages his/her intentions in altering the data or transmission of the data.
- Authentication: This allows the sender and receiver to confirm their identity and the origin/destination of the information.

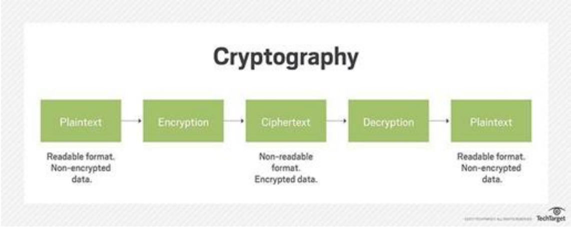
Cryptography
Plaintext
Encryption
Ciphertext
Decryption
Plaintext
Readable format. Non-encrypted data.
Non-readable format. Encrypted data.
Readable format. Non-encrypted data.
TechTarget

Fig. 1. Cryptography

The information that is to be encrypted by the sender before the transmission is written in plaintext. Plaintext is a term used in cryptography which is nothing but the information that is readable by the user (human being) before being encrypted by the computer. Plaintext is encrypted into ciphertext using cypher algorithm. Ciphertext is the result obtained after the encryption of the plaintext using algorithms called “cipher”. Ciphertext isn't to be confused with code text because the latter is used to encrypt the data using codes and not cipher. In order to encrypt and decrypt any information “KEY” is required. Now what is a key? A key is the most basic, important and essential component in cryptography. It is basically a big number used to provide desirable properties like encryption and decryption of information, confidentiality, integrity, and authentication. The length of the key is measured by the number of binary digits (“bits” - i.e, 1’s and 0’s) it takes to represent it’s value. Keys are usually in hundreds or in some cases a few thousand bits long. This provides a fine balance between security and computational efficiency. If the key is too short, and the key is not secure(weak), too long, and it makes the process slow, these keys are typically generated in computer systems using softwares that generates random numbers. This type of key generation is used for encrypting and decrypting data of day-to-day use, as it provides less adequate keys which may seem too weak to stop third party entities to access information of utmost importance. For critical information it is preferable to generate and store keys inside Hardware Security Modules (HSM). One of the methods used to generate such keys is the Chinese Remainder Theorem (CRT). It uses a set of residue modulus to provide the bits from the remainder. This process works only on positive integers that are relatively prime. The modulo operation provides a remainder by dividing one positive integer with another. For the CRT to provide us with the necessary keys, it is important that only positive co-prime numbers are fed into the system (meaning the CRT works only for positive integers that are co-prime in nature). What are coprime numbers? Any two numbers are said to be coprime if their highest common factor (Greatest common divisor) is 1. For example, the coprime numbers to 12 are 1, 5, 7, 11, 13, 17, 19, 23, 25 and so on. There are many other ways we can use that provide us with the same output like Fermat’s Theorem, Euler’s Theorem, Euclid’s Algorithm and many more. But these algorithms are time consuming, complex in structure and to implement and are used to solve integers of lower values, whereas Chinese Remainder Theorem is easier to implement with reduced number of steps and can compute larger numbers faster compared to the other methods. There are many applications and advantages in using the chinese remainder theorem algorithm - some of them are - Password Reconstruction, Encoding given data (secret sharing), Biometric Cryptosystem, to compute the distributed factors, Lagrange interpolation method, Fast Fourier transform and many more. Using Chinese remainder theorem, we are implementing WINOGRAD’s small convolution algorithm. This algorithm computes the convolution of numbers with reduced number of multiplication and addition steps, thus reducing the overall complexity of the process. Winograd’s algorithm can be used to compute cyclic convolution as linear convolution by reducing it using modulo $P^n - 1$, the cyclic convolution can be calculated using chinese remainder theorem with $(P) = P^n - 1$, which is much simpler.

2. Literature survey

Wenjie Wang, Xiang-Gen Xia. “A Closed-Form Robust Chinese Remainder Theorem and Its Performance Analysis”.

This paper talks about the ways the Chinese Remainder Theorem constructs and integers from its multiple reminders that are not robust meaning that a small error in the remainder may cause a large error in the reconstruction. The traditional CRT works only when all the moduli are co-prime. The robust CRT proposes a necessary and sufficient condition on the remainders to obtain the desired closed-form output. These closed-form robust CRT algorithms are used in both theoretical analysis and numerical simulations. The results show that the demonstrates closed-form output obtained has a much simpler performance

ZHANG Yun-peng, LIN Xia, WANG Qiang, “Asymmetric Cryptography Algorithm with Chinese Remainder Theorem”

This paper talks about the asymmetric algorithm based on Chinese Remainder Theorem and double sequence. Double sequence uses the sequence of random numbers that generate from the interference of Logistic and Chebychev chaotic mapping to interfere with the backpack sequence. This sequence is done while setting the easy solutions of SUPER INCREASING knapsack problem as the limitations of the algorithm. CRT is used to hide the sequence mentioned above before transforming into modulus the hidden backpack sequence. With the help of simulations and comparisons, this algorithm is excellent with higher efficiency and better security.

Lein Harna1, Miao Fuyoub2 “Multilevel threshold secret sharing based on the Chinese Remainder Theorem”

This paper talks about the generalization of classical threshold of Multilevel threshold secret sharing (MTSS). In MTSS the shareholders are classified into various security subsets. The threshold value of a higher level subset is smaller than the threshold value of a lower level subset. A shareholder’s share in a higher level subset can be used as a share in a lower level subset to recover the secret. Chinese Remainder Theorem (CRT) is one of the popular tools used in designing Secret-Sharing. A unique feature in this design is that each shareholder needs to keep one private share. The proposed scheme in this paper is based on the Asmuth-Bloom’s secret-sharing which is unconditionally secure.

Xiang-Gen Xia and Kejing Liu “A Generalized Chinese Remainder Theorem for Residue Sets with Errors and Its Application in Frequency Determination from Multiple Sensors with Low Sampling Rates.”

This paper talks about how Chinese Remainder Theorem (CRT) has been generalized from determining a single integer from its remainders to determine multiple integers from their sets of remainders. The first step is to obtain sufficient conditions on the number of incorrect residue sets, so that multiple integers can be uniquely determined. from their residue sets. Next we apply the newly proposed algorithm to multiple frequency determination from multiple sensors with low sampling rates and show the effectiveness of the proposed algorithm.

Sonali S. Mhatre, Vandana B. Salve, “Enhanced Chinese Remainder Theorem based Broadcast Authentication in Wireless Networks”

This paper talks about how wireless networks make extensive use of broadcast messages. All routing and network management activities must depend on the broadcast authentication mechanisms to ensure that data is being originated from a valid source. The main aim of this work is to provide an efficient scheme for sensor network broadcast authentication by considering different properties of broadcast authentication. A protocol called ENHANCED CHINESE Remainder theorem based on broadcast authentication (ECRTBA) is proposed for wireless sensor networks. An important feature of this scheme is that it makes use of the concept of independent keys that support infinite rounds of broadcasts and also provides instant authentication with no need of buffering.

Johann Groszschaed “The Chinese Remainder Theorem and its Application in a High-speed RSA Crypto Chip.”

This paper talks about the multiplier architecture of the RSA crypto-chip. The RSA crypto-chip is a high-speed hardware accelerator used for long integer modular arithmetic. Performance of RSA hardware is predominantly determined by an efficient implementation of the long integer modular arithmetic and the ability to utilize the CRT for the private key operations. Popular crypto-systems like the RSA Encryption Scheme [RSA78], The Diffie-Hellman(DH) Key Agreement Scheme [DH76], Digital Signature Algorithm(DSA) [mat941] are based on long integer modular exponentiation. A crucial difference between the RSA scheme and crypto-system based on the discrete logarithm problem is the fact that the modulus used in RSA encryption scheme is the product of two prime numbers. This utilizes the CRT in order to speed up the private key operations. From a mathematical point of view, the use of CRT for RSA decryption is well known. For hardware implementation, a special multiplier architecture is necessary to meet the requirements for efficient CRT based decryption.

3. Methodology used

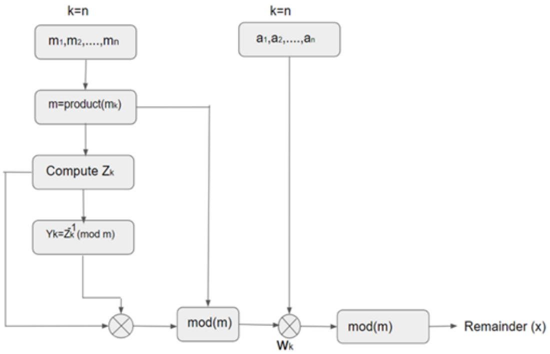

Fig. 2. Block diagram of Chinese remainder theorem algorithm

The above designed block diagram is the representation of the chinese remainder theorem that provides us the remainder of any two given coprime numbers. Using the above algorithm, the process becomes simpler and easier to obtain the remainder with the help of modular arithmetic. Our simultaneous congruence’s will be,

$$X \equiv a_1(\text{mod } m_1) \equiv a_2(\text{mod } m_2) \equiv a_3(\text{mod } m_3)$$

our objective is to obtain the W_k component. From the given numbers, the mod component and the number component is split; Z and the Y components are obtained. Product of all ‘m’ components is found out and the Z and Y components are product modulated and multiplied with the product(m) component. The product obtained is multiplied with the number component to obtain the W component. This W component is multiplied with the mod(m) component to obtain the remainder X.

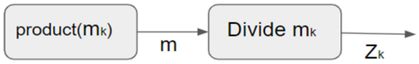

Fig. 3. Block diagram of computation of Z_K

This block diagram is a representation of how the Z component is obtained. Here, all the mod components are multiplied to provide a product term [product(m)]. This product term is divided by each of the individual mod components to obtain the Z component

i.e,

Z_K= m / m_K

where, k= number of terms.

k=1,2,3….n

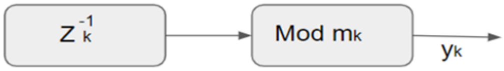

Fig. 4. Block diagram to compute Y_K

This block diagram is the representation of the Y component obtained. Here, the obtained Z component is made inverse and multiplied with the mod(m) component to obtain the Y component. [the inverse of Z component can be found out by using Euclid’s extended algorithm],

i.e, $Y_{\boldsymbol{K}} = Z_K^{-1}(\text{mod } m_K)$ (1)

where, k= number of terms.

k=1,2,3….n

Now , to obtain the W_K component , the Z and Y obtained components are multiplied with the mod(m) component.

i.e, $W_K = Z_K Y_K(\text{mod m})$ (2)

where, k= number of terms.

k=1,2,3….n

‘m’ = product of all the m_K components.

4. Hardware components

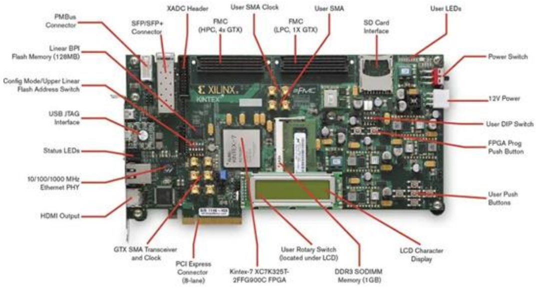

Fig. 5. Kintex7

The KC705 evaluation board for the Kintex®-7 FPGA issues a hardware environment for developing and evaluating designs targeting the Kintex-7 XC7K325T-2FFG900C FPGA. The KC705 board issues features known to many embedded processing systems, including a DDR3 SODIMM memory, an 8-lane PCI Express® interface, a tri-mode Ethernet PHY, general purpose I/O, and a UART interface. Other features can be added by using FPGA Mezzanine Cards (FMCs) attached to either of two VITA-57 FPGA mezzanine connectors issued on the board. High pin count (HPC) and low pin count (LPC) FMCs are provided.

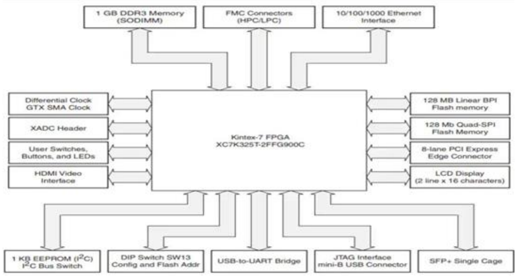
1 GB DDR3 Memory (SODIMM)
FMC Connectors (HPC/LPC)
10/100/1000 Ethernet Interface
Differential Clock GTX SMA Clock
XADC Header
User Switches, Buttons, and LEDs
HDMI Video Interface
Kintex-7 FPGA XC7K325T-2FFG900C
128 MB Linear BPI Flash memory
128 Mb Quad-SPI Flash Memory
8-lane PCI Express Edge Connector
LCD Display (2 line x 16 characters)
1 KB EEPROM (I2C) I2C Bus Switch
DIP Switch SW13 Config and Flash Addr
USB-to-UART Bridge
JTAG Interface mini-B USB Connector
SFP+ Single Cage

Fig. 6. Electrostatic Discharge Caution (EDC)

Prevention of ESD damage:

- Use an ESD wrist or ankle strap and ensure there is skin contact. Connect the equipment end of the strap to an unpainted metal surface on the chassis.
- Avoid touching the adapter against your clothing. The wrist strap protects components from ESD on the body.
- Handle the adapter by its bracket or edges only. Avoid touching the printed circuit board or the connectors.
- Put the adapter down only on an anti-static surface such as the bag supplied in your kit.
- If you are returning the adapter to Xilinx Product Support, place it back in its anti-static bag immediately.

5. Software components

Cadence Design System is the software component used.

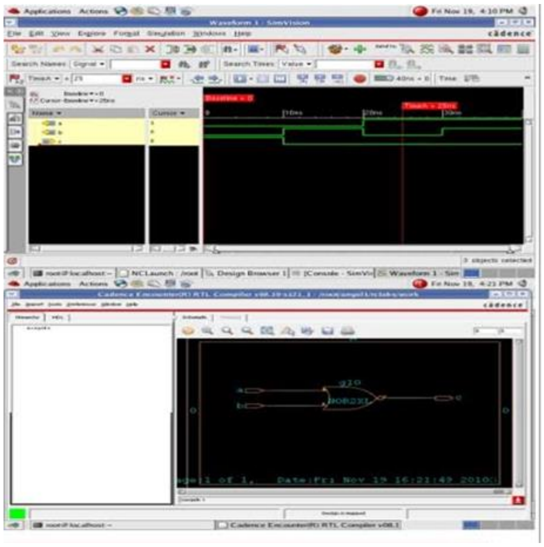

Fig. 7. Cadence software

6. Conclusion

From the mentioned literature reviews we are able to collect enough data to help us provide suitable knowledge in performing Winograd's Algorithm using the Chinese remainder theorem.

References

[1] Wenjie Wang, Xiang-Gen Xia, "A Closed-Form Robust Chinese Remainder Theorem and Its Performance Analysis", IEEE Transaction on signal processing, Vol. 58, No. 11, November 2010.
[2] Zhang Yun-Peng, Lin Xia, Wang Qiang, "Asymmetric Cryptography Algorithm with Chinese Remainder Theorem", 2011.
[3] Lein Harna, Miao Fuyoub, "Multilevel threshold secret sharing based on the Chinese Remainder Theorem", September 2014.
[4] Xiang-Gen Xia and Kejing Liu. "A Generalized Chinese Remainder Theorem for Residue Sets with Errors and Its Application in Frequency Determination from Multiple Sensors with Low Sampling Rates". IEEE signal processing letters, vol. 12, No. 11, November 2005.
[5] Sonali S. Mhatre, Vandana B. Salve, "Enhanced Chinese Remainder Theorem based Broadcast Authentication in Wireless Networks", 2012.
[6] Johann.Groszschaed1. "The Chinese Remainder Theorem and its Application in a High-speed RSA Crypto Chip", IEEE 2000.
[7] Carles Ferrer, "A Secure Algorithm for Inversion Modulo 2K," September 2018.
[8] Shaoqiang Bi and Warren J. Gross, "The Mixed-Radix Chinese Remainder Theorem and Its Applications to Residue Comparison", December 2008.
[9] Yuke Wang, "New Chinese Remainder Theorems". May 2007.
[10] Artur Jakubski, "Selected application of the Chinese remainder theorem in multiparty computation", April 2006.
[11] Xiang-Gen Xia and Genyuan Wang, "Phase Unwrapping and A Robust Chinese Remainder Theorem", April 2007.
[12] Laszlo Hars, "Modular Inverse Algorithms Without Multiplications for Cryptographic Applications", March 2005.
[13] Joppe W. Bos, "Constant Time Modular Inversion", August 2014.
[14] Saurabh Singh, "Use of Chinese Remainder Theorem to generate random numbers for cryptography", September 2010.
[15] Xingyu Liu, "Pruning of Winograd and FFT Based Convolution Algorithm", April 2005.