VLSI Implementation of Rsa Encryption and Decryption Method Using Montgomery Modular Multiplier

K.Geetha Devi [1], Dr.V.R.Vijaykumar [2]
[1](Dept Of Electronics And Communication Engineering, Anna University Engineering College, Anna University,Coimbatore)
[2](Dept Of Electronics And Communication Engineering, Anna University Engineering College,Anna University,Coimbatore),
Associate Professor,Department Of The Head

Abstract: *The Rivest Shamir And Adleman (Rsa) Encryption And Decryption Algorithm Is Used The Performance In Popular Public Key Cryptosystem For Mutual Authenticate.The Main Step Used In The Algorithm Is Modular Exponentiation Which Can Be Done By A Sequence Of Modular Multiplication. The Modular Multiplication Is The Major Factor, In Many Crypto Systems,The Rsa Two-Key System And In The Proposed Digital Signature Standard Dss. One Of The Most Efficient Algorithm Of Modular Multiplication Is The Montgomery Multiplication.Modified Radix-4 Modular Multiplication Was Developed Based On Montgomery Multiplication Technique.Carry Select Adder With Technique Of Scg, Fsc, Hsg To Avoid, Carry Propagation, Delay, And Also Reduced The Area, Which Present A Very Fast Algorithm Was Presented And Used For Computing Modular Reduction.Minimized Of Power, Delay And Area.Vlsi Design Of A Configurable Rsa Public Key Cryptosystem Supporting The 1024-Bit Based On Montgomery Algorithm Achieving Comparable Clock Cycles Of Current Relevant Works But With Smaller Die Size.*

Keywords: *Decryption,Encryption,Carry Select Adder,Montgomery Multiplier,Mutual Authentication.*

I. Introduction

Rsa Is A Widely Used Cryptosystem In The World. It Is A Public Key Cryptosystem Which Uses Two Kinds Of Key, Private Key And Public Key. Every User Has Both Of The Keys, A Private One And A Public One. If User A Wants To Send A Message To B, He Need B's Public Key To Encrypt The Message. After Encrypted, The Message Is Received By B, Then B Uses His Private Key To Decrypt The Message.Rsa Algorithm Can Be Classified As Three Algorithms, The Key Generation Algorithm, Encryption Algorithm, And Decryption Algorithm. Rsa Algorithm Is A Cryptographic Algorithm Introduced By Ron Rivest, Adi Shamir And Leonard Adleman. Rsa Implemented Following Two Important Ideas:1. Public-Key Encryption: In Rsa, Encryption Keys Are Made Public While The Decryption Keys Are Kept Private, So Only The Person With The Correct Decryption Key Can Decipher An Encrypted Message. Everyone Has Their Own Encryption And Corresponding Decryption Keys. The Keys Are Made In Such A Way That The Decryption Key Cannot Be Easily Deduced From The Public Encryption Key.

2. Digital Signatures: Signature Can Be Verified By Anyone, Using The Corresponding Public Encryption Key. Signatures Therefore Cannot Be Copied. Also, No Signer Can Later Deny Having Signed The Message. The Various Steps Involved In Rsa Algorithm.In Modular Arithmetic Computation, Montgomery Modular Multiplication, More Commonly Referred To As Montgomery Multiplication, Is A Method For Performing Fast Modular Multiplication. Given Two Integers *A* And*b* And Modulus *N*, The Classical Modular Multiplication Algorithm Computes *Ab* Mod *N*. Montgomery Multiplication Works By Transforming *A* And *B* Into A Representation Known As Montgomery Form. For A Modulus *N*, The Montgomery Form Of *A* Is Defined To Be *A R* Mod *N* For Some Constant *R* Depending Only On *N* And The Underlying Computer Architecture. If *Ar* Mod *N* And *B R* Mod *N* Are The Montgomery Forms Of *A* And *B*, Then Their Montgomery Product Is *Ab R* Mod *N*. Montgomery Multiplication Is A Fast Algorithm To Compute The Montgomery Product. Transforming The Result Out Of Montgomery Form Yields The Classical Modular Product *Ab* Mod *N*. Montgomery Multiplication Algorithm Is The Most Efficient Algorithm Available. The Main Advantage Of Montgomery Algorithm Is That It Replaces The Division Operation With Shift Operations. During Two Decades Many Alternative Forms Of Montgomery Algorithms Are Introduced. These Architectures Use Carry Save Addition.

The Work Presented Two Types Of Montgomery Algorithms Which Use Carry Save Adder (Csa). One Of The Two Types Used Four-To Two Csa And The Other Used Five-To-Csa. They Had Given A Brief Comparison Between These Two Versions Of Montgomery Multipliers. They Had Found That The Multiplier Using Four-To-Two Csa Architecture Has Shorter Critical Path Than That Of Five-To-Two Csa Multiplier. The

Proposed Csla Adder Is A Variable Length Csla Adder And Based On This Proposed Csla We Are Creating The 256 Bit Sqrt- Csla Structure. This Sqrt Csla Adder Is Reducing The Delay Of The Architecture. The Proposed Csla Is Design With Variable Length Inputs, So It's Flexible To Different Application.

The Proposed Csla Structure Is As Shown In Fig.8. It Is Composed Of One Half-Sum Generation (Hsg) Unit, One Full Sum Generation (Fsg) Unit, One Carry-Generation (Cg) Unit, And One Carry-Selection (Cs) Unit. The Cg Unit Composed Of Two Units Namely Cgo And Cg 1 Corresponding To Input-Carry '0' And '1', Respectively. Input To The Hsg Unit Is Two N-Bit Operands A And B And Outputs Are Half-Sum (Hs) Word So And Half-Carry (Hc) Word Co Of Width N-Bit Each. Cg Unit Receives Both So And Co From Hsg Unit And Gives Two N-Bit Full-Carry Words Co, And C1, Corresponds To Carry-Input '0' And '1' ,Respectively. The Carry Selection Unit Selects Final Carry Based On The Cin From Two Anticipated Carry Words C^0_1 And C^1_1 If Cin = 0 Then It Selects Co I; Otherwise It Selects C^1_1cout Is The Msb Of C Obtained From Cs Unit And Remaining (N-L) Lsbs Of Cs Unit Are Xo Red With (N-L) Msbs Of Half-Sum (So) In The Fsg Unit To Obtain Final-Sum.

II. Review Of Literature

2.1 High Speed Rsa Implementation Based On Modified Booth's Technique And Montgomery's Multiplication

S. S. Ghoreishi, H. Bozorgi, Has Proposed High Montgomery's Multiplication For Fpga Platform, Rivest, Shamir And Adleman (Rsa) Encryption Algorithm Is One Of The Most Widely Used And Popular Publickey Cryptosystem. The Main Step In This Algorithm Is Modular Exponentiation Which Can Be Done By A Sequence Of Modular Multiplication. Thus, Modular Multiplication Is The Major Factor, In Many Cryptosystems,The Rsa Two-Key System And In The Proposed Digital Signature Standard Dss. One Of The Most Efficient Algorithms Of Modular Multiplication Is The Montgomery Multiplication. In This Paper, Modified Radix-4 Modular Multiplication Was Developed Based On Booth's Multiplication Technique. We Use Csa (Carry Save Adder) To Avoid Carry Propagation. Also A Very Fast Algorithm Was Presented And Used For Computing The Modular Reduction. We Proposed New Hardware Architecture For Optimum Implementation Of This Algorithm.

2.2 An Optimized Hardware Architecture For The Montgomery Multiplication Algorithm

Tenca And Ko C, In Montgomery Modular Multiplication Is One Of The Fundamental Operations Used In Cryptographic Algorithms, Such As Rsa And Elliptic Curve Cryptosystems. At Ches 1999, Tenca And Ko¸C Introduced A Now-Classical Architecture For Implementing Montgomery Multiplication In Hardware. With Parameters Optimized For Minimum Latency, This Architecture Performs A Single Montgomery Multiplication In Approximately 2n Clock Cycles, Where N Is The Size Of Operands In Bits. In This Paper We Propose And Discuss An Optimized Hardware Architecture Performing The Same Operation In Approximately N Clock Cycles With Almost The Same Clock Period. Our Architecture Is Based On Pre-Computing Partial Results Using Two Possible Assumptions Regarding The Most Significant Bit Of The Previous Word, And Is Only Marginally More Demanding In Terms Of The Circuit Area.

2.3 Analyzing and Comparing Montgomery Multiplication Algorithms

Burton S. Kaliski, Jl,In This Paper Discusses Several Montgomery Multiplication Algorithms, Two Of Which Have Been Proposed Before. We Describe Three Additional Algorithms, And Analyze In Detail The Space And Time Requirements Of All Five Methods. These Algorithms Have Been Implemented In C And In Assembler. The Analyses And Actual Performance Results Indicate That The Coarsely Integrated Operand Scanning (Cios) Method, Detailed In This Paper, Is The Most Efficient Of All Five Algorithms, At Least For The General Class Of Processor We Considered. The Montgomery Multiplication Methods Constitute The Core Of The Modular Exponentiation Operation Which Is The Most Popular Method Used In Public-Key Cryptography For Encrypting And Signing Digital Data.

2.4 Fast Montgomery Modular Multiplication And Rsa Cryptograpic Processor Architechture

Omar Nihouche, Mokhtar Nibouche, New Generic Silicon Architectures For Implementing Montgomery's Multiplication Algorithm Are Presented. These Use Carry Save Adders (Csas) To Perform The Large Word Length Additions Required By This Algorithm When Used For Rsa Encryption And Decryption. It Is Shown That Using A Four-To-Two Csa With Two Extra Registers Rather Than A Five-To-Two Csa Leads To A Useful Reduction In The Critical Path Of The Multiplier, Albeit At The Expense Of A Small Increase In Circuitry.

2.5 Hardware Implementation of a Montgomery Modular Multiplier in A Systolic Array

Siddika.Bernaors, Lejla.Batina, In This Paper Describes A Hardware Architecture For Modular Multiplication Operation Which Is Efficient For Bit-Lengths Suitable For Both Commonly Used Types Of Public Key Cryptography (Pkc) I.E. Ecc And Rsa Cryptosystems. The Challenge Of Current Pkc Implementations Is To Deal With Long Numbers (160-2048 Bits) In Order To Achieve System's Efficiency, As Well As Security. Rsa, Still The Most Popular Pkc, Has At Its Root The Modular Exponentiation Operation. Modular Exponentiation Consists Of Repeated Modular Multiplications, Which Is Also The Basic Operation For Ecc Protocols. The Solution Proposed In This Work Uses A Systolic Array Implementation And Can Be Used For Arbitrary Precisions. We Also Present Modular Exponentiation Based On The Montgomery's Multiplication Method (Mmm).

2.6 An Efficient Csa Architechture For Montgomery Modular Multiplication

Zheng Li, Lei Yang, The Montgomery Multiplier Is Implemented Using Verilog Language And Synthesized By Leonardo Spectrum Tool For Fpga Technology. Our Result Shows That The Multiplier With 1024-Bit Operands Can Run At A Clock Of 114.2mhz And It Uses 4512 Slices. We Have A New Addition Approach To Perform The Result Format Conversion In Montgomery Modular Multiplication. Based On The New Approach, The Proposed Csa Architecture Has Much Better Performance Than Conventional Ones In Most Design Since The Critical Delay Of This Architecture Is $O(2)$ And The Number Of Clock Cycles Is Decreased. Using Only Two Csas, The Area Reduction Of The Montgomery Multiplier Is Very Significant.

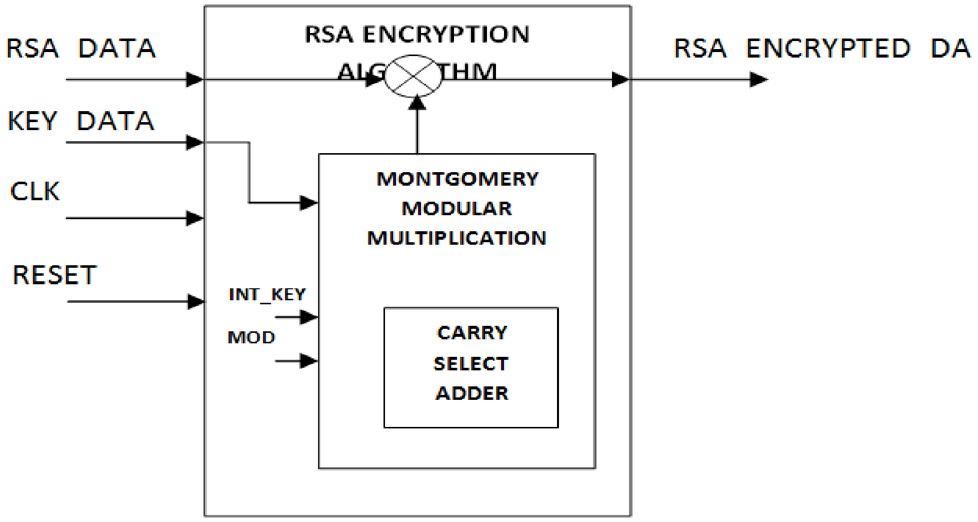

Fig: 1.1 Architecture Diagram Of Encryption And Decryption

III. Montgomery Modular Multiplier

3.1.Introduction

Montgomery Modular Multiplier Algorithm To Reduce The Critical Path Delay Of Montgomery Multiplier. In Addition, The Drawback Of More Clock Cycles For Completing One Multiplication Is Also Improved While Maintaining The Advantages Of Short Critical Path Delay. This Algorithm Avoids Long Chains Of Carry Propagation, And Therefore Speeds Up Both The Modular Multiplication And Squaring Operations Required During The Exponentiation Process. Many Rsa Implementations Are Bit-Serial Based Structures. Using 128 Bits To Simulate The Program Of Montgomery Multiplier For Encryption. A New Scs-Based On The Bases Of Critical Path Delay Reduction, Clock Cycle Number Reduction, And Quotient Pre-Computation Reduction. The Bit-Parallel Approach Presents A Solution That Overcomes The Speed Problems Of Many Systems . Unfortunately, This Solution Comes With Its Own Drawback, As It Requires An Important Area-Usage. And Pin-Out, Which May Not Be Satisfied In The Resource-Limited Fpga Chips.For Applications For Which The Bit-Serial Approach Is Slow And The Bit-Parallel One Is Faster Than Required And Occupies A Large Area, A Trade Off Must Be Found **.**

3.2 Advanced Montgomery Modular Multiplier

A New Scs-Based Montgomery Montgomery Multiplier Algorithm Using One-Level Parallel Prefix Adder Architecture Is Proposed To Significantly Reduce The Required Clock Cycles For Completing One Mm.As Shown In Scs-Mm-New Algorithm Will Be Shown Below, Which Varies From A Single Bit To The

Word-Length, Is Referred To As The Digit Size. Since The Digit Size Is Variable, The Digit Approach Provides The Designer With A Flexible And Efficient Area-Time Method To Find The Speed And The Area That Match The Designs.

Since The Digit Size Is Variable, The Digit Approach Provides The Designer With A Flexible And Efficient Area-Time Method To Find The Speed And The Area That Match The Designs.The Rsa Algorithm Is A Secure, High Quality, Public Key Algorithm. It Can Be Used As A Method Of Exchanging Secret Information Such As Keys.

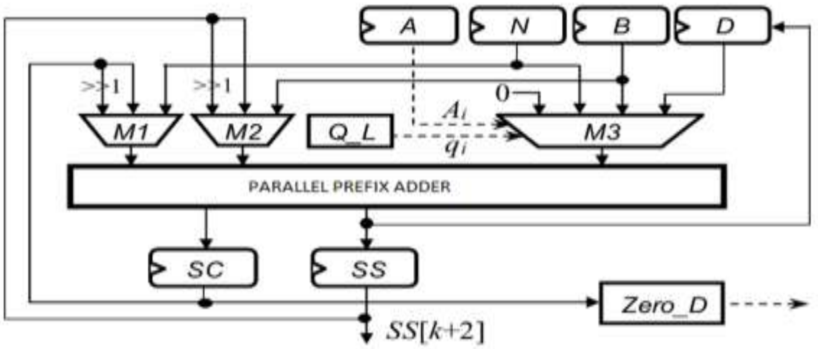

Figure 1.2 Modified Scs Based Montgomery Multiplication

3.3 Scs Based Montgomery Multiplier

The Serial Approach Processes The Data Serially Where At Exert Clock Cycle A Single Data Bit Is Fed To The Rsa Processor To Be Processed.Incontrast,The Parallel Approach Processes The Data Bits In A Parallel Fashion In Just One Clock Cycle.

Many Rsa Implementations Are Bit-Serial Based Structures**.** This Is Essentially Due To Their Design Simplicity And Low Hardware Area-Usage Requirements. However. When High Sample Rates Are Required. The Family Of Bit-Serial Architectures Leads To A Slow System Speed**.** To Avoid This Problem, And Thus, Reach Higher System Speed, It Is Clear That A Move Towards Higher Bit-Width Operations Is Necessary.

Authentication By A Client Usually Involves The Server Giving A Certificate To The Client In Which A Trusted Third Party Such As Verisign Or Thawte States That The Server Belongs To The Entity (Such As A Bank) That The Client Expects It To.Authentication Does Not Determine What Tasks The Individual Can Do Or What Files The Individual Can See. Authentication Merely Identifies And Verifies Who The Person Or System.

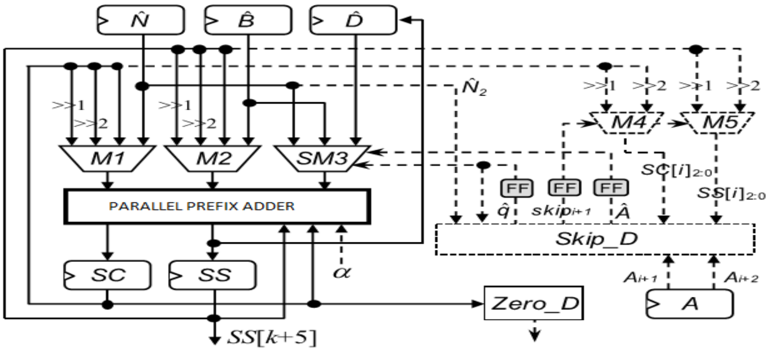

Figure 1.3 Proposed Scs Based Montgomery Multiplier

IV. System Implementation

4.1 Authentication

Authentication Is Used By A Server When The Server Needs To Know Exactly Who Is Accessing Their Information Or Site. Authentication Is Used By A Client When The Client Needs To Know That The Server Is System It Claims To Be. In Authentication, The User Or Computer Has To Prove Its Identity To The Server Or Client.Usually, Authentication By A Server Entails The Use Of A User Name And Password. Other Ways To Authenticate Can Be Through Cards, Retina Scans, Voice Recognition, And Fingerprints.

4.2 Carry Select Adder

The Proposed Csla Adder Is A Variable Length Csla Adder And Based On This Proposed Csla We Are Creating The 256 Bit Sqrt- Csla Structure. This Sqrt Csla Adder Is Reducing The Delay Of The Architecture. The Proposed Csla Is Design With Variable Length Inputs, So It's Flexible To Different Application. The Proposed Csla Structure Is As Shown In Fig.8. It Is Composed Of One Half-Sum Generation (Hsg) Unit, One Full Sum Generation (Fsg) Unit, One Carry-Generation (Cg) Unit, And One Carry-Selection (Cs) Unit. The Cg Unit Composed Of Two Units Namely Cgo And Cg 1 Corresponding To Input-Carry '0' And '1', Respectively.Input To The Hsg Unit Is Two N-Bit Operands A And B And Outputs Are Half-Sum (Hs) Word So And Half-Carry (Hc) Word Co Of Width N-Bit Each. Cg Unit Receives Both So And Co From Hsg Unit And Gives Two N-Bit Full-Carry Words Co, And C1, Corresponds To Carry-Input '0' And '1' ,Respectively.

V. Result

Rsa Implementation Based Booth Multiplier Technique To Montgomery With Carry Select Adder Technique And Shown The Performance Of Rsa Implementation With Encryption With 128 Bits Based Multiplier Using Rsa Algorithm. Each Verilog Programs Included As Carry Save Adder,Full Adder,Montgomery Multiplier And Rsa Montgomery Multiplier 128 Used For The Simulation Works On Xilinx 14.2.Implementation Of 128-Bit Encryption Was Done. By Using 128 Bits Area,Time,Power Can Be Reduced. We Synthesized Our Design And Showed That 128-Bit Rsa Encryption Is Performed On Chip Device Is 0.538 Ms.The Results Of The Encryption For A 128-Bit Block Of Data Were Presented. Carry-Save Format To Escape From The Format Conversion, Leading To Fewer Clock Cycles But Larger Area Than Scs-Based Multiplier. To Enhance The Performance Of Montgomery Mm While Maintaining The Low Hardware Complexity.

VI. Conclusion

In This Paper Has Modified The Scs-Based Montgomery Multiplication Algorithm And Proposed A Low-Cost And High-Performance Montgomery Modular Multiplier. The Proposed Multiplier Used One-Level Csa Architecture And Skipped The Unnecessary Carry-Save Addition Operations To Largely Reduce The Critical Path Delay And Required Clock Cycles For Completing One Mm Operation. We Use Csa (Carry Save Adder) To Avoid Carry Propagation. Also A Very Fast Algorithm Was Presented And Used For Computing The Modular Reduction.The Rsa Algorithm Is A Secure, High Quality, Public Keyalgorithm. It Can Be Used As A Method Of Exchanging Secret Information Such As Keys And Producing Digital Signatures The Rsa Algorithm Is Very Computationally Intensive,Operating On Very Large (Typically Thousands Of Bits Long) Integers.

Acknowledgement

I Would Like To Express My Gratitude To My Guide Dr.V.R.Vijayakumar.,M.E.,Ph.D(,Department Of The Head) For Guiding Me Properly In My Project Work And For Helping To Solve The Project Work Difficulties. I Would Also Like To Thanks All The Staff Members Of Electronics And Communication Engineering Department For Supporting Me And Guiding Me In My Project Work Whenever Required.

References

[1] T. Blum And C. Paar,(2001), 'High-Radix Rsa Montgomery Modular Exponentiation On Reconfigurable Hardware'vol.5, No. 7, Pp-70-77.

[2] V. Bunimov, M. Schimmler, And B. Tolg,(2002) 'A Complexity-Effective Version Of Montgomery's Algorihm' Vol.15,No.16,Pp-71-81.

[3] S.-R. Kuang, J.-P. Wang, K.-C. Chang, And H.-W. Hsu,(2013) 'Energy-Efficient High-Throughput Montgomery Modular Multipliers For Rsa Cryptosystems' Vol.8,No.2,Pp-25-37.

[4] C. Mcivor, M. Mcloone, And J. V. Mccanny, (2004),'Modified Montgomery Modular Multiplication And Rsa Exponentiation Techniques' Vol.8,No.2,Pp-29-38.

[5] Miyamoto, N. Homma, T. Aoki, And A. Satoh,(2011), 'Systematic Design Of Rsa Processors Based On High-Radix Montgomery Multipliers' Vol.4,No.4,Pp-367-371.