FPGA based data security

Deepali Pagire, M. M. Jadhav
SCOE, Pune-41

Abstract

Information security has assumed a significant importance in today's world, especially because minor breaches can lead to major risks in the fields of national security and other e-commerce applications and transactions. This necessitates implementing cryptographic algorithms in hardware to achieve better security and faster response as opposed to any software implementation. A promising solution combining high flexibility with the speed and physical security of traditional hardware is the FPGA. The main purpose in cryptography is to make message concept unintelligible. The performance of most crypto systems is primarily determined by an efficient implementation of arithmetic operations. When implementing public key cryptography such as RSA the primary requirements are high speed arithmetic computation, small size and low power consumption and resistance to side channel attacks. In this paper, the hardware implementation of the RSA cryptographic algorithm, which is a public key algorithm. This RSA algorithm depends on computation of repeated modular exponentiation.

1. Introduction

In this internet age, identity theft, intellectual property protection, and financial account and payment protection are key concerns to both consumers and designers. To keep everything safe, many systems employ security measures such as data encryption and physical shielding to prevent hackers and other malicious activities from accessing data, financial information, or even intellectual property. Even the simple car door entry key/ignition key has become more secure with embedded processors running challenge and response authentication to prevent vehicle theft. Furthermore, the movement to "smarten" the energy grid will also escalate the demand for secure communications to prevent hackers or terrorists from wreaking havoc on the power grid. Security of network communications is the most important issue in the world. Information transactions related to banks, credit cards, and government policies are transferred from place to place with the help of network transmission. The need for security arises when a group of people wants to achieve the identity of the person to whom you are talking. The need to be introduced to someone you do not know by someone you know or trust. It is important that if we exchange information, we can guarantee the origin and validity of this information. In private conversation to exchange information such a way that only the intended recipient of the information can actually read the information. The major fears of a security system denial of service, guessing or stealing passwords, theft of equipment, stupidity. Security is all about fulfilling these needs. With the spread of digital data around the world through the internet, the security of the data has raised a concern to the people. Many methods are coming up to protect the data from going into the hands of the unauthorized person. Secure transmission refers to the transfer of data such as confidential or proprietary information over a secure channel. The need for efficient and reliable digital data communication systems has been rising rapidly in recent years. This need has been brought on by a variety of reasons, among them being the increase in automatic data processing equipment and the increased need for long range communication.

Protecting one's property from other mortal beings is a basic human instinct. "Information" is one such property that has to be aptly protected from potential miscreants. The need and significance of information security is very old. There are two possible ways to safeguard one's data. One, you can conceal the message and hope that the enemy would not find it. Second, you scramble the data and hope that the enemy would not be able to unscramble it. The latter procedure is known as cryptography. Of course, the first method can be easily combined with cryptography as the data is first scrambled and then hidden, for extra security. The origin of cryptography can be traced back to the era of Julius Caesar when he came to know that his messages were intercepted on route. So he replaced every A to D, B to E and so on. Only someone who knew "Shift by 3" could easily decipher it. This procedure is popularly known as "Caesar Cipher", and was used during Gallic wars. Cryptography is the German word, which literally means Secret Writing. Before digital communication came into existence, cryptography was used by military for espionage. Its use became widespread as it became imperative for business to make sure that sensitive data was transferred from one point to another in an airtight secure manner through public networks. With technological advancement and reduced costs, the common mass has been able to reach out for this technology.

So, what is Cryptography? Cryptography is the application of mathematical tools and techniques related to information security such as integrity, confidentiality, authentication, etc. It is an art of guarding transmitted information from unauthorized interception or tampering. It involves translating information of any kind (text, pictures, sound, and so on) into standard form of transmission, and protecting this information against distortion by ransom noise. The need for information security is become inevitable due to rapid development and applications of computer networks and internet technology. Information needs to be secure as they are valuable resources of any organization like other resources such as hardware, software, employee, financial resources and legal position. Security consists of some policies, rules, protocols and standards that help the organization to meet the objectives and missions. Organizations need security to protect their assets from illegal and unauthorized access, also people in their personal life need to keep confidential their private documents, family albums and films. Physical security and access control is a solution but it is not enough. Electronic data are easy to access, steal or copy via networks, so we need more secure methods to keep them safe. Cryptography is the art or science encompassing the principles and methods of transforming an intelligible message (plaintext) into one that is unintelligible (ciphertext) and then retransforming that message back to its original form. In modern times, cryptography is considered to be a branch of both mathematics and computer science, and is affiliated closely with information theory, computer security and engineering. The three most important objectives of cryptography include (1) confidentiality, (2) data integrity, and (3) authentication. Confidentiality refers to the protection of information from unauthorized access. An undesired communicating third party (called adversary) must not be able to access the communication material. Data integrity ensures that information has not been manipulated in an unauthorized way. Finally, Authentication is the equivalent of a signature and studied in two concepts: entity authentication and message authentication. Protection of a cryptographic module within a security system is necessary to maintain the confidentiality and integrity of the information protected by the module. This standard specifies the security requirements that are to be satisfied by a cryptographic module.

2. Literature review

In the digital world, data is the heart of computer communication and global economy. To ensure the security of the data, the concept of data hiding has attracted people to come up with creative solutions to protect data from falling into wrong hands. Digital data can be delivered over computer networks from one place to another without any errors and interference. Security associated between the two end communicating nodes – the source and the destination. Since a pair of nodes chooses to employ a secure communication scheme, their ability to authenticate each other is indispensable. The trust relationship can be instantiated, for example, by the knowledge of the public key of the other communicating end. Encryption has long been used by militaries and governments to facilitate secret communication. Encryption is now commonly used in protecting information within many kinds of civilian systems, for some of their data in storage. Spatial encryption technique for secured transmission of data in networks. The algorithm is designed to break the ciphered data packets into multiple data which are to be packaged into a spatial template. A secure and efficient mechanism is provided to convey the information that is necessary for obtaining the original data at the receiver-end from its parts in the packets. An authentication code (MAC) is also used to ensure authenticity of every packet. The application developed for end to end secure transmission of the SMS. The algorithm used is Advanced Encryption Standards algorithm[1]. This application is developed on Android platform and is one of a kind. The later part of the paper explains the working of SMS.

The RSA algorithm is a secure, high quality, public key algorithm. The RSA algorithm is a secure, high quality, public key algorithm. A hardware implementation of RSA encryption scheme has been proposed by Deng Yuliang & Mao Zhigang. in [2], where they use Montgomery algorithm for modular multiplication. A similar approach has been taken by C. N. Zhang & Y. Xu. in [3]. J. Fry, and M. Langhammer [6] proposed method for low cost FPGA implementation of RSA. This design scheme focuses on the implementation of a RSA cryptographic processor using Bit-Serial Systolic Algorithm. Sushanta Kumar Sahu & Manoranjan Pradhan[7] have used multiple key sizes for implementing on fpga using shift &add algorithm.

3. Algorithm

Cryptography is the science of protecting clear, meaningful information using mathematical algorithms. Using common encryption algorithms, cryptography provides support for multiple security services to protect the information. Security Services such as digital signature and data confidentiality can be provided by Cryptography. Multiple algorithms may be used to protect information with cryptography.

RSA is a cryptosystem, which is known as one of the first practicable public-key cryptosystems and is yet widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977. A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message.

After picking a public exponent *d* and by finding a prime *p*, make those two values public. Using the extended Euclidean algorithm, determine *e*, the inverse of the public exponent modulo j (ϕ) = *p*-1. When people want to send someone a message C, they can encrypt and produce cipher text A by computing A = C^dmod *p*. To recover the plain text message, someone compute C = A^e mod *p*. But the private key *e* is the inverse of *d* modulo *p*-1. Since *p* is public, anyone can compute *p*-1 and therefore determine *e*. RSA algorithm solves the above problem by using an Euler's multiplicative phi-function. If *p* and *q* are relative prime, then ϕ (*pq*) = ϕ (*p*) ϕ (*q*). Hence, for primes *p* and *q* and *n* = *pq*, ϕ (*n*) = (*p*-1)(*q*-1). The problem is finding *e* that satisfies *d***e* = 1 mod (*p*-1)(*q*-1) where the pair (*n*,*d*) is the public key and *e* is the private key. The prime p and q must be kept secret or destroyed. To compute cipher text A from a plain text message C, find A = C^d mod *n*. To recover original message, compute C = A^e mod *n* . Only the entity that knows *e* can decrypt. Because of the relationship between *d* and *e*, the algorithm correctly recovers the original message C, since A^emod *n* =C^{de} mod *n* = C1mod *n* = C mod *n*. To know ϕ (*n*) one must know *p* and *q*. In other words, they must factor *n*. Multiplying big prime numbers can be a one-way function. Factoring takes a certain number of steps, and the number of steps increases sub-exponentially as the size of the number increases. Extended Euclidean algorithm can be used to find private key *e*.

The difficult part of RSA encryption/decryption lies on the modulus calculation of $c = m^e \ mod \ n$, to get the encrypted message "*c*". To calculate the encrypted message "*c*", it involves exponentiation that requires large amount of combinational logic, which increases exponentially with the number of bits being multiplied and exponentiation is separated into a number of multiplications and squaring. Each multiplication can be realized by a series of additions.

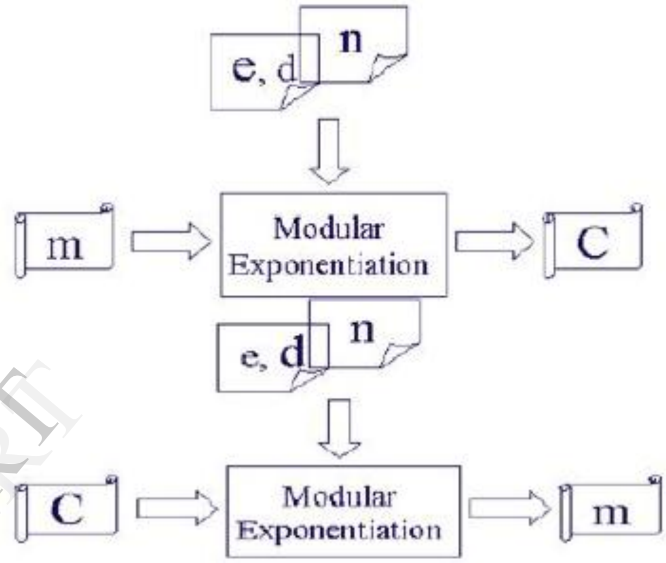

Figure.1 RSA Encryption and Decryption Structure.

4. FPGA

The Spartan3 family of Field-Programmable Gate Arrays is specifically designed to meet the needs of high volume, cost-sensitive consumer electronic applications. The eight-member family offers densities ranging from 50,000 to 5,000,000 system gates. The Spartan-3 family builds on the success of the earlier Spartan-IIE family by increasing the amount of logic resources, the capacity of internal RAM, the total number of I/Os, and the overall level of performance as well as by improving clock management functions. Numerous enhancements derive from the Virtex-II platform technology. These Spartan-3 FPGA enhancements, combined with advanced process technology, deliver more functionality and bandwidth per dollar than was previously possible, setting new standards in the programmable logic industry. Because of their exceptionally low cost, Spartan-3 FPGAs are ideally suited to a wide range of consumer electronics applications, including broadband access, home networking, display/projection and digital television equipment.

The Spartan-3 family is a superior alternative to mask programmed ASICs. FPGAs avoid the high initial cost, the lengthy development cycles, and the inherent inflexibility of conventional ASICs. Also, FPGA programmability permits design upgrades in the field with no hardware replacement necessary, an impossibility with ASICs. Low-cost, high-performance logic solution for high-volume, consumer-oriented applications, densities up to 74,880 logic cells, selection interface signaling, up to 633 I/O pins, 622+ Mb/s data transfer rate per I/O, 18 single-ended signal standards, 8 differential I/O standards including LVDS, RSDS, termination by Digitally Controlled Impedance, signal swing ranging from 1.14V to 3.465V, double Data Rate (DDR) support, DDR, DDR2 SDRAM support up to 333 Mb/s, logic resources, abundant logic cells with shift register capability, wide, fast multiplexers, fast look-ahead carry logic, dedicated 18 x 18 multipliers, JTAG logic compatible with IEEE 1149.1/1532, select RAM hierarchical memory, up to 1,872 Kbits of total block RAM, up to 520 Kbits of total distributed RAM, digital Clock Manager (up to four DCMs), clock skew elimination, frequency synthesis, high resolution phase shifting, eight global clock lines and abundant routing.

5. Conclusion

With the ever increasing necessity of computer security, it is time that industry starts looking for ways to ensure data integrity from within. Due to creative exploits, even internal system information may be compromised, which can result in an unauthorized user taking control of an entire system. This plays a prominent role in today's world where things such as the power grid, air traffic control and nuclear reactors could be abused to affect millions of people worldwide by a simple vulnerability such as a buffer-overflow. One answer to this growing threat is an RSA based internal encryption scheme for return addresses on the stack. If it is found feasible to implement, this solution would ensure that over 90% of the modern computer infiltrations are stopped. This one project will have profound consequences for security systems worldwide, and will allow system administrators to have another means of protection in their network implementation. This will provide a base-level analysis of the usefulness of an RSA based encryption approach. Even if RSA is not found to be sufficiently fast, researchers will at least have the ability to know that a different method should be implemented.

6. References

[1] R. Rivest, A. Shamir, L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of theACM, vol. 21 (2), pp. 120-126, 1978.
[2] Deng Y., Mao Z., and Ye Y.,. 1998. Implementation of RSA Crypto-Processor Based on Montgomery Algorithm.
[3] Zhang. C.N, Xu. Y and Wu. C., 1997. A Bit-Serial Systolic Algorithm and VLSI Implementation for RSA.
[4] B. Schneier, Applied cryptography, second edition, NY: John Wiley &Sons, Inc., 1996.
[5] L. Scripcariu, M.D. Frunza, "A New Character Encryption Algorithm", Proceedings of the Intern. Conference on Microelectronics and Computer Science, Chisinau, (Republica Moldova), ICMCS 2005, ISBN 9975-66- 040-1, pp. 83 - 86, Sept. 15-17, 2005.
[6] J. Fry, and M. Langhammer, "FPGAs Lower cost for RSA yptography."
[7] Sushanta Kumar Sahu &Manoranjan Pradhan , 2011. FPGA Implementation of RSA Encryption System , International Journal of Computer Applications (0975 – 8887)Volume 19– No.9, April 2011
[8] Cryptography and network security – William Stallings
[9] www.rsasecurity.com
[10] William Stallings, "Cryptography and Network Security Principles and Practice",Fifth edition,2011
[11].FPGA Compiler II /FPGA Express VHDL Reference ManualVersion 1999.05, May 1999
[12] www.xillinx.com
[13].Stephen Brown,"Fundamentals of digital logic design", Second edition, 2007
[14].Douglas L Perry, "VHDL Programming by example", Fourth edition, 2010