A Highly Secured FPGA Based CryptoProcessor

Prathibha T, Ashwini K B

Abstract—The impotance of security in electronic data transaction has acquired an essential relevance during the last few years. In this sense, cryptography techniques are especially applicable. In this paper, a field programmable gate array(FPGA) based approach is used three algorithms namely 128 bit advanced encryptionnstandard(AES), River-Shamir-Adleman(RSA) and secure Hash Algorithm(SHA-1). These crypto subsystems scramble data into unreadable text which can be only being decrypted by party those possesses the associated key which provides confidentiality. Along with this digital signature operation is performed which provides authentication and integrity.

Index Terms— Certification authority, Cryptograpic system, Digital signature,Hashing function,Information security.

1 INTRODUCTION

Information security is a fundamental requirement for an operational information society. Although issues considered as information security, such as secrecy of messages, privacy of communication, and reliable authentication, to name a few, have been important throughout history, developments in digital computing and information technology have set new requirements and challenges for them. The importance of information security has grown because new technologies have made accessing and misusing confidential information easier and more profitable. Hence, information security, previously considered mostly by militaries and governments, has become an issue having relevance even for an average person living in a modern information society because of its significance in commerce, communication, etc. Cryptography is an effective way of protecting sensitive information as it is stored on media or transmitted through network communication paths [1].

The hackers can lead attacks against software or hardware implementations for a lower cost. In such cases, implementation can be the weak part of the encryption process. Thus security should be considered at different levels of abstraction, from technology to application. Without a whole consideration of these levels, and links between the levels, weaknesses can easily and quickly appear in the considered devices.

In this paper, a secure crypto hardware is proposed to provide the data security as well as database. These schemes apply 128-bit Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), and Secure Hash Algorithm (SHA) module.

.

2 SECURITY SCHEME

- *Prathibha T, Assistant Professor, electronics and communication engineering in channabasaveshwara Institute of Technology,Gubbi, India, PH-08131-223818. E-mail: prathibha.t@cittumkur.org*
- *Ashwini K B, Assistant Professor, electronics and communication engineering in channabasaveshwara Institute of Technology,Gubbi, India, PH-08131-223818. E-mail: ashwini.kb@cittumkur.org.*

Some of the cryptographic algorithms can only perform encryption, whereas others can perform digital signatures and encryption. When hashing is involved, a hashing algorithm is used, not an encryption algorithm. It is important to consider that all encryption algorithms cannot necessarily provide all security services. Most of these algorithms are used in some type of combination to provide all the necessary security services required of an environment such as

- A message can be encrypted, which provides confidentiality.
- A message can be hashed, which provides integrity
- A message can be digitally signed, which provides authentication and integrity.
- A message can be encrypted and digitally signed, which provides confidentiality, authentication, and integrity.

Therefore in this paper three algorithms are considered namely AES, RSA and SHA-1.

2.1 ADVANCED ENCRYPTON SYSTEM

AES is more specifically a symmetric block cipher [6]. This means that it operates at a block of data, instead of a single element per iteration which could be a bit or a byte. AES is also known as Rijndael. Actually AES is just a variant of Rijndael. The algorithm is composed of three main parts: Cipher, Inverse Cipher and Key Expansion. Cipher converts data to an unintelligible form called cipher text while Inverse Cipher converts data back into its original form called plain text. Key Expansiongenerates a Key Schedule that is used in Cipher and Inverse Cipher procedure. Cipher and Inverse Cipher are composed of specific number of rounds.

AES is able to encrypt and decrypt a block of data using a key. The key and the block of data (from now on, the input) have a fixed length. The input is always 128-bit (16 bytes), while the key can be 128-bit, 192-bit or 256-bit (16, 24 and 32 bytes respectively) and AES algorithm is applied to data 10, 12, or 14 times which is also known as "rounds" respectively making it highly secure.

2.2 RIVEST-SHAMIR-ADLEMAN

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 [10]. 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 needs B's public key to encrypt the message. After encrypted, the message is received by B, and then B uses his private key to decrypt the message. The RSA schemes used in this paper are as follows:

Encryption: Encryption is done always with public key. In order to encrypt with public key it need to be obtained. Public key must be authentic to avoid man-in-the middle attacks in protocols. Verifying the authenticity of the public key is difficult. When using certificates a trusted third party can be used. If certificates are not in use then some other means of verifying is used (fingerprints, etc). The message to be encrypted is represented as number m, 0<m<n-1. If the message is longer it need to be spitted into smaller blocks. Compute $c = m^e \bmod n$, where the e and n are the public key, and m is the message block. The c is the encrypted message.

Decryption: The private key (d) is used to decrypt messages. Compute: $m = c^d \bmod n$, where n is the modulus (from public key) and d is the private key.

RSA digital signatures/verification scheme: Digital signatures are always computed with private key. This makes them easily verifiable publicly with the public key. The raw message m is never signed directly. Instead it is usually hashed with hash function and the message digest is signed. This condition usually also means that the message m in fact is not secret to the parties so that each party can compute the message digest separately. It is also possible to use so called redundancy function instead of hash function. This function is reversible which makes it possible to sign secret messages since the message can be retrieved by the party verifying the signature. In practice hash function is often used.

2.3 Secure Hash Algorithim-1

A SHA-1 is a hash function which takes a variable sized input message and produces a fixed-sized output. The output is usually referred to as the hash code or the hash value or the message digest. Since a message digest depends on all the bits in the input message, any alteration of the input message during transmission would cause its message digest to not match with its original message digest. This can be used to check for forgeries, unauthorized alterations, etc.

SHA1 hashing algorithm outputs a 160bit digest of any sized file or input[7]. In construction it is similar to the previous MD4 and MD5 hash functions, in fact sharing some of the initial hash values. It uses a 512 bit block size and has a maximum message size of 2^{64} -1 bits. The description of SHA1 Algorithm consists of a 6-step process of padding of '1000...', appending message length, preparing 80 process functions, preparing 80 constants, preparing 5 word buffers, processing input in 512 blocks.

2.4 Digital ignature

A digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, and that it was not altered in transit.Because only the message digest is signed, the signature is usually much shorter than the data that was signed [7].

A hash function, as itself, does not do anything of immediate high value, but it is a very important building block for other algorithms. For instance, they are used with digital signature.

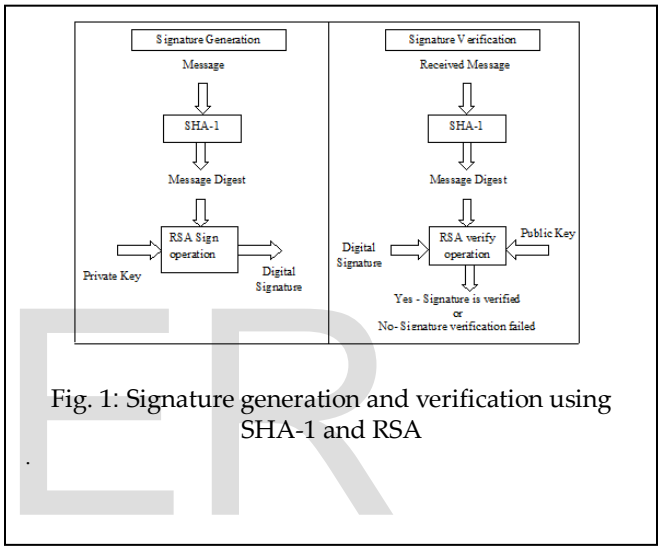

Fig. 1: Signature generation and verification using SHA-1 and RSA

In the RSA digital signature process, the private key is used to encrypt only the message digest. The encrypted message digest becomes the digital signature and is attached to the original data. Fig. 1 illustrates the basic RSA Data Security digital signature process. To verify the contents of digitally signed data, the recipient generates a new message digest from the data that was received, decrypts the original message digest with the originator's public key, and compares the decrypted digest with the newly generated digest. If the two digests match, the integrity of the message is verified. The identity of the originator also is confirmed because the public key can decrypt only data that has been encrypted with the corresponding private key.

3 SECURITY SYSTEM OVERVIEW

Cryptography is a method of storing and transmitting data in a form that only those it is intended for can read and process it. First it converts any data in its original form, called the plaintext, into an incomprehensible form, known as the cipher text. This process is called encryption. The reverse process of recovering the plaintext from the cipher text is called decryption. Cryptography is an effective way of protecting sensitive information as it is stored on media or transmitted through

network communication paths.

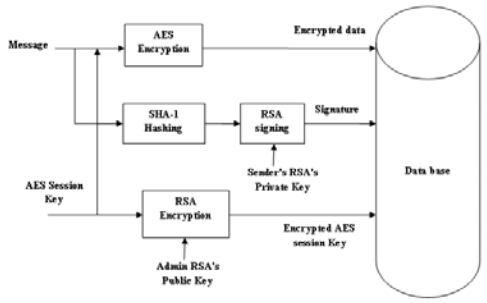

Fig. 2(a): Saving Medical Data into Database

.

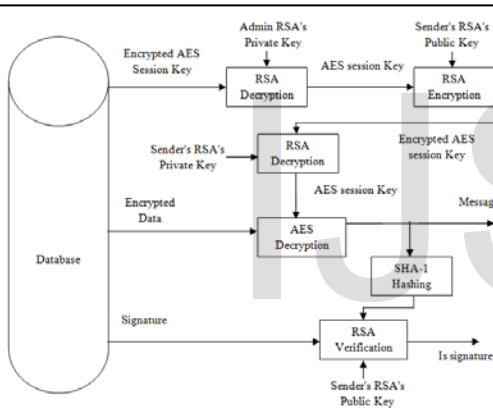

Fig. 2(b): Retrieving Medical Data from Database

.

Figure 2 illustrates the high-level system overview which provide data security three operations are performed in this project namely, encryption of a message, generating Signature of a sender and encrypting session key.

In this application, each person is assigned to a personal computer with their unique crypto hardware module and cryptographic keys, in this case we assume the third party software, like certificate authority (CA) distributed the crypto hardware with cryptographic keys. Therefore, each entity has a unique crypto hardware and RSA private key and shares a common AES session key. The user's public key that is associated with the private key stored in the crypto hardware.

Referring to the Fig.2(a), the message which need to be stored in database is encrypted using AES. To encrypt the message by AES it needs session key which is maintained secretly by the user and the encrypted message is stored in the database. In this 128 bit AES session key is used. At the same time the message is sent to the SHA-1 to produce hash code. The hash code of the message is encrypted with the sender's private key using RSA, which generates the signature for the message. This signature also stored in the database. The AES session key is encrypted and stored in database using RSA by a Admin's public key.

Referring to the Fig.2(b), during message retrieving process from database, the encrypted AES session key is first decrypted with Admin's RSA private key. If anyone hack the Admin's private key means message can be easily hacked without bothering about sender public or a private key. So the decrypted AES session key is again encrypted by the Admin using desired sender's public key before transmit it to that person. Now the encrypted session key is decrypted by the sender's private key. This is used to decrypt the message by the AES decryption. Now to check the signature decrypted message has to be sent to the SHA-1 hashing to generate the message digest and then sent to the RSA verifier to verify signature with the sender's public key. If this is valid then message recovered is correct.

4 HARDDWARE-SOFTWARE DESIGN

The coding was done using VHDL as the hardware description language. The code was simulated using ModelSim software. VHDL synthesis tools can create logic-circuit structures directly from VHDL behavioral descriptions, and target them to a selected technology for realization. Using VHDL, we can design, simulate, and synthesize anything form a simple combinational circuit to a complete microprocessor system on a chip. The Synthesis, place and route was performed using Xilinx ISE. VHDL started out as documentation and modeling language, allowing the behavior of digital-system designs to be precisely specified and simulated [8, 9] and language specification allows multiple modules to be stored in a single text file.

5 CONCLUSION

The present work focuses on to provide confidentiality, authenticity, integrity, and nonrepudiation services. A message can be encrypted using AES and digitally signed using SHA-1 and RSA, which provides confidentiality, authentication, and integrity. AES session key is also encrypted and stored in database using RSA by a public key so that key and the message both are protected. This enables the transmission of confidential information over insecure channels without unauthorized disclosure.

REFERENCES

[1] Crowe F., Daly A., Kerins T., and Marnane W. (2004). Single-Chip FPGA Implementation of a Cryptographic Co-processor. Department of Electrical & Electronic Engineering, University College Cork. UnpublishedW.-K. Chen.

[2] Diffie, W., and Hellman, M. New Directions in Cryptography. IEEE Transactions on Information Theory, November 1976.

[3] Khalil M. and Hau Y., W., An Embedded Cryptosystem Implementing Symmetric Cipher and Public-Key Crypto Algorithms In Hardware. University Technology Malaysia. M.Sc. Thesis, 2005.

[4] Khalil, Hau Y., W., Paniandi A., "Design and Implementation of a Private and Public Key Crypto Processor for Next-Generation IT Security Application", Malaysian Journal of Computer Science, Vol. 19(1), 2006, 29-45

[5] Khalil M. and Iliasaak Ahmad. A Customizable Cryptographic Service Provider for an Embedded Cryptohardware System.Universiti Teknologi Malaysia: M.Sc. Thesis, 2007.

[6] NIST, (2001a) Announcing the Advanced Encryption Standard (AES), FIPS PUBS 197, NIST

[7] NIST, (2001b) Secure Hash Standard. FIPS PUB 180-2, NIST

[8] NIST, (2001c) A Statistical Test Suite for Random and Pseudorandom Number Generator For Cryptographic Application. NIST Special Publication 800-22. NIST.

[9] NIST, (2007) Recommendation For Key Management – Part 1 (Revised), NIST Special Publication 800-57. NIST:

[10] Rivest R.L, Shamir.A, and Adleman.L. (1978). A Method for Obtaining Digital Signature and Public-Key Cryptosystems, Comm. in ACM, 21:120-126.

[11] Subhayan S., Sk. Iqbal H., Kabirul I., Dipanwita R. C., P Pal C., (2003) Cryptosystem Design for Embedded System Security Proceedings of the 16th International Conference on VLSI Design (VLSI'03), IEEE

[12] Vaudenay S., (2006), A Classical Introduction To Cryptography, Springer.