DESIGN AND IMPLEMENTATION OF CRYPTOGRAPHIC CO-PROCESSOR USING VHDL FOR BIOMEDICAL APPLICATION

Dr. M. Dhamodaran¹, K.P. Ramya Meenakshi², V. Shivanya², N.Swetha²

¹Professor,²UG Student

Department of Electronics and Communication Engineering, M.Kumarasamy College of Engineering, Karur, India

E-mail dhamodarammune@gmail.com

ABSTRACT

Data protection (confidentiality, honesty, credibility, and non-repudiation) is crucial in today's world, where our lives are fully reliant on the internet. As a result, stronger encryption methods are constantly in demand. Because of this factor, Information systems must be encrypted in order to protect data and resources from malicious actions. Crypto algorithms are at the heart of such security systems. Cryptography is a series of techniques for encrypting data using special algorithms that render the data unreadable to the naked eye until decrypted using predefined algorithms by the sender. Various cryptographic algorithms can be used to implement a cryptographic coprocessor. Such an algorithm must strike a balance between processing time, storage space, robustness, and security level. As a result, we've proposed a cryptographic co-processor based on the MD5 hashing algorithm. On the ModelSim software, we have implemented our processor in VHDL.

Data protection mainly used in biomedical communications.

Keywords: Cryptography, Message Digest Algorithm-5, Encryption, biomedical, VHDL.

I. INTRODUCTION

A crypto-processor is a special processor that helps with encryption. It secures data transmission by encrypting and decrypting messages. A crypto processor based on cryptographic algorithms can be used in a wide range of electronic devices, including PCs, PDAs, security subsystem hardware, and removing the need for physical security measures to secure the rest of the subsystem. The receiver decrypts the encrypted message using a key that we use is either the different as or same from the sender's key and retrieves the original message. People without the right key would be unable to read the message even if they stole the decrypted version. The art of encrypting data by translating it into an unreadable format known as cipher text. Cryptography is the name given to this method. Cryptography is the ancient science of encrypting data such that only the sender and recipient can decrypt it. The message can only be decoded into plain text by those who have a private key. Email messages, corporate records, and credit card details are all encrypted using cryptography. Cryptography systems can be divided into two types: Public-key crypto systems use two keys: a public key shared by all and a private key shared only by the message's recipient. Symmetric-key systems use a single key shared by both the sender and the receiver. The recipient and sender of any data share a single, identical key for encrypting and decrypting the data in this encryption scheme. Public-key cryptography, on the other hand, encrypts and decrypts data using two keys: a public key for encryption and a private key for decryption. Symmetric-key systems are quick and simple to use, but they have the disadvantage of requiring all parties to exchange the key in a secure manner. Public-key 2 encryptions prevent this problem because the public key can be exchanged insecurely and the private key is never transmitted[1]. The general method of public key cryptography also involves encryption and decryption. Method of Encryption is the converting data (plaintext) into an algorithm (cipher) that makes it unreadable to anyone but those with special knowledge (key). The method generates encrypted data as a result (cipher text). Decryption is the method of restoring the readable state of encrypted data (converts the cipher text to plaintext using an algorithm called decipher). Military and government agencies have long used encryption to promote secret communication. However, it is now widely used to secure data in transit or storage in a variety of civilian systems. As a result, cryptographic processing has been elevated to the foreground of device growth. The Message Digest Algorithm-5 is the most important Hashing algorithm nowadays (MD5).
We begin with plaintext, or unencrypted data, in cryptography. Plaintext is encrypted into cipher text, which is then decrypted back into accessible plaintext (in most cases). To encrypt and decrypt data, a cryptographic scheme is used, as well as some sort of key. This method is often written as: for those who like formulas.

\[ P = D_k (C) \]
\[ C = E_k (P) \]

Where \( P \) denotes plaintext, \( C \) denotes cipher text, \( E \) denotes encryption, \( D \) decryption, and \( k \) denotes key. There are some other functions that crypto can support, as well as some words that you may hear: Perfect Forward Secrecy (also known as Forward Secrecy): Even if the server storing the messages is hacked, this function prevents past encrypted sessions from being breached. This is accomplished by creating a separate key for each session, ensuring that a single key compromise does not complicate the communications as a whole. Perfect Security: A device that cannot be broken because the cipher text reveals nothing about the plaintext or the key. To achieve perfect security, the key must be at least as long as the plaintext, making analysis and even brute-force attacks impossible. One example of a device like this is one-time pads. Message Repudiation (also known as Deniable Authentication): A mechanism by which participants in a message exchange can be confident of the messages' validity while also allowing senders to plausibly deny their involvement to a third party [2-3].

Symmetric Cryptography: In symmetric cryptography, data is encrypted and decrypted using a single key. This is a private encryption key. This encryption technique's drawback is that the private key can only be shared by the registered sender and recipient. The most commonly used symmetric key Data Encryption System is a type of cryptography system (DES).

Asymmetric Cryptography: For encryption and decryption, asymmetric cryptography employs a pair of keys: a public key and a private key. A sender can use their public key to encrypt data, and the recipient can use their private key to decrypt it. This approach solves the problem of key distribution.

Cryptographic Hashes: A person's left thumb fingerprint is the same every time it's taken, but finding another person with the same left thumb fingerprint is difficult. Apart from her left thumb fingerprint, the fingerprint does not reveal any details about the individual. Just looking at person fingerprint, you can't tell what math skills she has or what eye color person has. A cryptographic hash is a digital fingerprint of a file. You use a computer programmed called a cryptographic hash function to generate a cryptographic hash of a file. Consider the following scenario: you want to build a cryptographic hash, or fingerprint, of your favorite cat picture. Hashing is a method of transforming a set of key values into a set of array indexes. To get a set of key values, we'll use the modulo operator Consider example of the hash table size 20, and also The (key, value) format is used for the objects [4-6].
II. METHODOLOGY

MD5 is a message processing hash calculation made by Rivest in 1992. It comprises of five stages (for additional subtleties, kindly allude to). The calculation used to deal with the message is at the core of MD5. The calculation is separated into four adjusts, each with 16 stages. The calculation is completed as follows: The estimations of A, B, C, and D are at first saved as impermanent factors. At that point each stage activity is rehashed multiple times. There is a nonlinear capacity that relates to each adjust. At last, the brief constants' qualities are added to the calculation's qualities, and the outcomes are saved in Registers A, B, C, and D. The message condensation of M is put away in registers A, B, C, and D after all message blocks have been handled. Message M is part into 512-bit impedes, every one of which is prepared freely. There is no information reliance between the bits of info information. Therefore, the information way can be pipelined in 64 cycles. Figure 3 portrays the MD5 one-round activity. The MD5 information is kept consistent by the Const Unit. The information message block is put away in the registers, and a choice module chooses the appropriate response that relates to the estimation of Xk in each round. Turn left, viper, and nonlinear capacities make up FU, which is a combinational rationale. MD5 (Message-Digest calculation 5) is a 128-bit cryptographic hash work that is regularly utilized in cryptography. MD5 has been utilized in a wide scope of safety applications as an Internet standard (RFC 1321), and it is regularly generally used to check the respectability of records. A 32-digit hexadecimal number is utilized to mirror a MD5 hash. MD5 is a strengthened variation of MD4. MD5 was obviously utilized as the model for SHA-1, as it imparts a few similitude’s to MD4. MD5 and SHA-1 are the two most normally utilized hash calculations today, yet MD5's ubiquity will die down as it is presently viewed as broken [7 -9].

2.1 ALGORITHM:

RFC 1321 portrays the MD5 hash and incorporates a C execution. MD5 is a hash that is indistinguishable from MD4. The cushioning and introduction are no different either way. MD5 works for 32-cycle words. Allow M to represent the message that should be decoded. The message M is adjusted to have a length (in bits) of 448 modulo 512, or 64 pieces not exactly a various of 512. A solitary 1 bit goes before the cushioning, which is trailed by enough zeros to cushion the message to the fitting length. Regardless of whether the length of M equivalents 448 mod 512, cushioning is as yet utilized. As an outcome, cushioning is available in at any rate the slightest bit and up to 512 pieces. The message's length (in bits) (prior to cushioning) is then added as a 64-bit block. The cushioned message is a different of 512 pieces, making it a various of 32 pieces also. Leave N alone the quantity of 32-cycle words in the (cushioned) code, and M be the message. N is a numerous of 16 because of the cushioning. The message digest is registered utilizing a four-word cushion (A, B, C, D). Every one of the registers A, B, C, and D is a 32-cycle register. The accompanying hexadecimal qualities are utilized to instate these registers:

A). Append padding bits: The primary move is to cushion the b-bits message (contribution) to make it 448 pieces in length, modulo 512. At the end of the day, the message ought to be just 64 pieces shy of being a different of 512, that is, the message in addition to 64 pieces ought to be distinguishable by 512 in the wake of cushioning. Reminder 0 will be (Message+64)/512.Padding is always done, regardless of the size of the post. A '1' bit is applied to the message first, followed by a sequence of '0' bits. For eg, if our message is 400 bits long, we'll add one '1' bit and 47 '0' bits to make 448 bits, which is 64 bits short of 512. If our message is 1200 bits long, we'll add one '1' bit and 271 '0' bits to it. This gives us a total of 1472 pieces. The sum of 1472 and 64 is divisible by 512. The original message is padded or expanded by at least 1 bit and up to 512 bits.

B). Append length: Presently we'll take the first message and change it into a 64-bit portrayal of the b-bit message. This is added to the past advance's presentation. The message is presently either precisely separable by 512 or a different of 512 long. This is multiple times distinct. The message is isolated into 512-cycle blocks at this stage. Each 512-cycle block is isolated into 16 of 32-digit words. M [0.....N1], where N is a numerous of 16, is the manner by which we signify the terms [10-12].

C). Initialize MD buffer: MD5 employs a four-word buffer, each of which is 32 bits long. A, B, C, and D are the letters we use to represent them.
Table 1: Setup the MD Buffer

<table>
<thead>
<tr>
<th>Word</th>
<th>01</th>
<th>23</th>
<th>45</th>
<th>67</th>
</tr>
</thead>
<tbody>
<tr>
<td>Word</td>
<td>89</td>
<td>Ab</td>
<td>Cd</td>
<td>ef</td>
</tr>
<tr>
<td>Word</td>
<td>fe</td>
<td>dc</td>
<td>ba</td>
<td>98</td>
</tr>
<tr>
<td>Word</td>
<td>76</td>
<td>54</td>
<td>32</td>
<td>10</td>
</tr>
</tbody>
</table>

D). Processing Message in 16 Block words: Two more helper functions are used. For instance, MD5 makes use of four auxiliary functions. Second, we employ a 64-element table.

![Hash Function Diagram](image)

**Fig 2: Initialize MD buffer**

![MD 5 Operation Diagram](image)

**Fig 3: MD 5 Operation**

We partitioned the message into 512-digit squares, and afterward each 512-bit block was isolated into 16 32-cycle words. \( M_{i} \) [0...Ki-1] signifies the 16 word (each 32-digit) blocks. Now we perform four rounds, each with 16 operations, for each word block. Every round follows the same basic pattern. Every round's operations are denoted by the letters [abcd]. The \( i \)-th value from the table \( k[i] \) is obtained using \( i \). \( i \) also denotes the total number of operations, which range from 0 to 64. The number of bits to move is denoted by the letter \( s \). We use array \( s \) to predefine shift values for each of the 64 operations[13-15].

2.2 CO-PROCESSOR:

Standard instructions and dedicated protection function units were provided by the coprocessor. VHDL is used to design and implement the coprocessor, but Verilog is used to implement the N-bit Adder in the ALU unit. We

www.turkjphysiotherrehabil.org
have used behavioral modeling to construct a register for memory initialization and synchronous read and write operations. Then we wrote test bench code for the entire cryptographic coprocessor to set acceptable input values for the input waveform. Finally, we simulated the waveform and double-checked our observations. The coprocessor's block diagram is as follows:

![Block Diagram](image)

**Fig 4: Proposed Method**

**Table 2: Comparison Table**

<table>
<thead>
<tr>
<th>Hash Algorithm</th>
<th>Time Elapse</th>
<th>Hash Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>MD5</td>
<td>0.01877 sec</td>
<td>32 digits</td>
</tr>
</tbody>
</table>

**III. RESULT AND DISCUSSION:**

Using the VHDL test bench, the cryptographic coprocessor in VHDL is finally tested. We have performed coding of various blocks and verified the simulation waveforms. The encryption is done by using MD5 algorithm in which the input of 32 bits and we got 128 bit output.

![Data Flow](image)

**Fig 5: Data Flow**
Numerous applications for crypto processors can be found in remote specialized gadgets, asset compelled gadgets like sensors, RFID labels, savvy cards, prepayment metering frameworks, banking, military applications, confined in registering, and safeguard zones, among others. Our proposed method of cryptographic co-processor works principally on MD5 hashing calculation which is irreversible. Hashing time is 6900 ns and therefore it works very fast as compared to symmetric and asymmetric cryptographic algorithms. The MD5 algorithm has solved the transmission and storage of plain code and other security issues with conventional passwords; however, it is vulnerable to collision and dictionary attacks. Using MD5 algorithm we can transmit the data for biomedical applications.

REFERENCES