IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 5, Oct-Nov, 2013
ISSN: 2320 - 8791
www.ijreat.org

Implementation of Elliptic Curve Cryptography in DSP 5416 Module

P.R.Lavanya[1], S.Anupriya[2] and Mr.N.Karthikeyan[3]

[1]Electronics and Communication Engineering, UG student, University College of Engineering, Ramanathapuram, Tamilnadu, India

[2]Electronics and Communication Engineering, UG student, University College of Engineering, Ramanathapuram, Tamilnadu, India

[3]Electronics and Communication Engineering, Asst Professor, University College of Engineering, Ramanathapuram, Tamilnadu, India

ABSTRACT

Cryptography is a science of writing a secret codes for the original message. It includes two processes namely encryption and decryption. An original message is known as the plaintext, while the coded message is called the ciphertext. The process of converting from plaintext to ciphertext is known as encryption; restoring the plaintext from the ciphertext is decryption. There are two types of cryptographic algorithms based on number of keys. They are symmetric (secret key cryptography) and asymmetric (public key cryptography).And our field of study is public key cryptography. There are lots of algorithms to implement public key cryptography. One of the commonly used algorithm is RSA algorithm. The drawback faced by RSA algorithm is the key length has increased over recent years and this has put a heavier processing load. To overcome this we like to implement Elliptic curve cryptography algorithm which has very small key length.

Key words:*Cryptography, ECC, Implementation, DSP 5416 Module*

1. INTRODUCTION

Cryptography provides techniques for keeping information secret, for determining that information has not been tampered with, and for determining who authored pieces of information. Cryptography is fascinating because of the close ties it forges between theory and practice, and because today's practical applications of cryptography are pervasive and critical components of our information-based society. Information-protection protocols designed on theoretical foundations appear in products and standards documents. The theoretical work refines and improves the practice, while the practice challenges and inspires the theoretical work. When a system is "broken," our knowledge improves, and next year's system is improved to repair the defect. A good cryptographer rapidly changes sides back and forth in his or her thinking, from attacker to defender and back. The current volume is a major contribution to the field of cryptography. It is a rigorous encyclopedia of known techniques, with an emphasis on those that are both secure and practically useful.

2. TYPES OF CRYPTOGRAPHIC ALGORITHMS

There are several ways of classifying cryptographic algorithms. For purposes of this paper, they will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. The three types of algorithms that will be discussed are:

2.1. Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption

2.2. Public Key Cryptography (PKC): Uses one key for encryption and another for decryption

2.3. Hash Functions: Uses a mathematical transformation to irreversibly encrypt information.

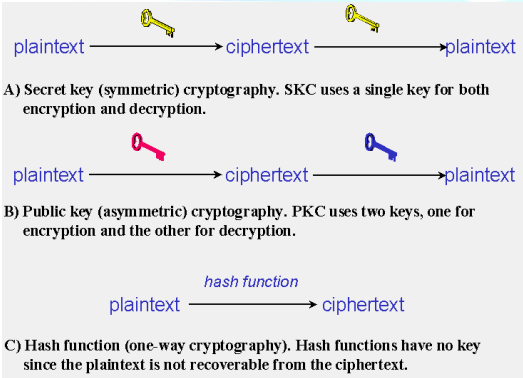

fig 1.1.Types of cryptographic algorithm

3. SYMMETRIC KEY VS PUBLIC KEY CRYPTOGRAPHY

3.1. Disadvantages of symmetric-key cryptography

1. In a two-party communication, the key must remain secret at both ends.

2. In a large network, there are many key pairs to be managed. Consequently, effective key management requires the use of an unconditionally trusted TTP.

3. In a two-party communication between entities A and B, sound cryptographic practice dictates that the key be changed frequently, and perhaps for each communication session.

4. Digital signature mechanisms arising from symmetric-key encryption typically require either large keys for the public verification function or the use of a TTP.

3.2. Advantages of public-key cryptography

1. Only the private key must be kept secret (authenticity of public keys must, however, be guaranteed).

2. The administration of keys on a network requires the presence of only a functionally trusted TTP as opposed to an unconditionally trusted TTP. Depending on the mode of usage, the TTP might only be required in an "off-line" manner,as opposed to in real time.

3. Depending on the mode of usage, a private key/public key pair may remain unchanged for considerable periods of time, e.g., many sessions (even several years).

4. Many public-key schemes yield relatively efficient digital signature mechanisms. The key used to describe the public verification function is typically much smaller than for the symmetric-key counterpart.

5. In a large network, the number of keys necessary may be considerably smaller than in the symmetric-key scenario.

4.ELLIPTIC CURVE CRYPTOGRAPHY

4.1. What is a Elliptic Curve

- Elliptic Curve (EC) systems as applied to cryptography were first proposed in 1985

independently by Neal Koblitz and Victor Miller.

- The discrete logarithm problem on elliptic curve groups is believed to be more difficult than the corresponding problem in (the multiplicative group of nonzero elements of) the underlying finite field.

  Advantage: compared with RSA ,it offer equal security for a smaller key size ,thereby reducing overhead.

4.2.Types of Elliptic Curves

Primary curve -best for software applications

Binary curve –best for hardware applications

4.3.Equation of elliptic curve

An elliptic curve over the real numbers is the set of points (x, y) that

$$y^2 = x^3 + ax + b$$

where x, y, a, and b are real numbers.

5. USING ELLIPTIC CURVES IN CRYPTOGRAPHY

The central part of any cryptosystem involving elliptic curves is the elliptic group. All public-key cryptosystems have some underlying mathematical operation. RSA has exponentiation (raising the message or ciphertext to the public or private values) ECC has point multiplication (repeated addition of two points).

6. KEY GENERATION IN ECC

1.Find Elliptic group of points $E_P(a,b)$

2. Pick a Base point G = (x,y) in Ep(a,b)

6.1.User A key Generation

Select Private Key n_A

Calculate Public P_A

$$P_A = n_A \times G$$

6.2. User B key Generation

Select private key n_B

Calculate Public P_B

$$P_B = n_B \times G$$

Generation of Secret key (session) by user A,

$$K = n_A \times P_B$$

Generation of Secret key (session) by user B,

$$K = n_B \times P_B$$

7. ENCRYPTION & DECRYPTION

Elliptic Curve Encryption

- Pm -> (x,y) Point message
- $Cm = \{ kG, Pm + k P_B \}$

  Cipher text consisting of pair of points.

  k-> random positive integer

Elliptic Curve Decryption:

$$Pm + k P_B - n_B(kG)$$

$$= Pm + k(n_B G) - n_B(kG)$$

$= Pm$-> Plain Text

8. APPLICATION OF ECC

- Wireless communication devices
- Smart cards
- Web servers that need to handle many encryption sessions
- Any application where security is needed but lacks the power, storage and computational power that is necessary for our current cryptosystem.

9. IMPLEMENTATION

We have implemented the Public key algorithm Elliptic Curve Cryptography in DSP 5416 module for the key size of 8 bits.

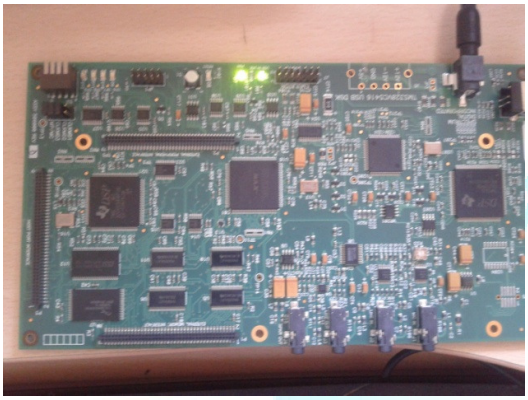

Fig 1.2 DSP 5416 module

10. CONCLUSION

During implementation of ECC algorithm we faced the problems of understanding the concepts of addition over prime curves and the improvement of key size for secure communication.

REFERENCES

[1]. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, Handbook of Applied cryptography, CRC press,August, 1996

[2] Certicom, The elliptic curve cryptosystem: an introduction to information
security [Retrieved October 3, 2003], www.certicom.com

[3] Certicom, Online ECC tutorial [Retrieved October 10, 2003],
www.certicom.com/resources/ecc tutorial/ecc tut 1 0.html

[4]Garrett, Paul. Making, Breaking Codes: An Introduction to Cryptology.
Prentice-Hall, 2001. [An undergraduate textbook on cryptography, includes
descriptions of ECC and NTRU.]

[5]J.Lopez and R. Dahab, "Improved algorithms for elliptic curve
arithmetic in GF(2n)," in Selected Areas in Cryptography, SAC'98,
ser. Lecture Notes in Computer Science, vol. 1556. Springer, 1999,

[6]Joseph H. Silverman, An Introduction to the
Theory of Elliptic Curves, June 19 { July 7, 2006}