ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2014

Flexible and an Efficient Hardware Architecture for A Secured Data Communication

G.M.Keerthi[1], M.Gopinath[2]

PG Scholar, ME VLSI Design, Angel College of Engineering and Technology, Tirupur, Tamilnadu, India[1]

Assistant Professor, Dept. of ECE, Angel College of Engineering and Technology, Tirupur, Tamilnadu, India[2]

ABSTRACT: Network Security is the most vital component in information security because it is responsible for securing the information among the networked computers. This paper analyzes the symmetric key and public key cryptographic techniques. The paper combines the characteristics of the AES and ECC for encryption standard. Implementation of encryption of the information is done in such a way that it will be impossible for the attackers to read the resources. In this method, conversion of text is done using AES algorithm and key will be encrypted using ECC algorithm. Result will be cipher which is decrypted on the receiver's side. This combined encryption methods enhance the speed and security.

KEYWORDS:Cryptography, Advanced Encryption Standard, Elliptic Curve Cryptography, Encryption, Decryption.

I. INTRODUCTION

Security processing is computation intensive, which normally includes lookup and fetching/updating of parameters (keys, encryption/authentication algorithms, initial values, and security-related protocol information), encryption and authentication, data transfer, bus contention resolution, etc. Powerful security processing architectures are thus important in high-speed network applications. Encryption algorithm is an important role for information security. Encryption is the process of transforming plaintext data into cipher text in order to secure its meaning and so preventing any unauthorized user from retrieving the original data. The Encryption has long been used by militaries and governments to facilitate secret communication. For technical reasons, an encryption scheme usually uses a pseudo-random encryption key generated by an algorithm. It is in principle possible to decrypt the message without possessing the key, but, for a well-designed encryption scheme, large computational resources and skill are required.

The Advanced Encryption Standard (AES) is the one among the symmetric key cryptographic algorithm which has been introduced to overcome the limitations of other algorithms like DES (Data Encryption Standard). The security of AES will be high due to the presence of large number of rounds or blocks and steps. The output of one block acts as the input of the next block in both encryption and decryption. For the wireless networks, this significantly is advantageous to the power needs. The elliptic curve cryptography is a type of symmetric key encryption method that is used for key exchange, digital signatures and also for encrypting the secure data. When compared to the other asymmetric key algorithms the system resource utilization like band width, memory, hard disk of this ECC is very much less. Therefore ECC is treated as the best suitable cryptographic algorithms for the wireless devices.

II. RELATED WORK

Wireless networks play critical roles in present work, home, and public places, so the needs of protecting of such networks are increased. Encryption algorithms play vital roles in information systems security. These symmetric algorithms consume a significant amount of computing resources such as CPU time, memory, and battery power. CPU and memory usability are increasing with a suitable rates, but battery technology is increasing at slower rate. This analyse the several encryption algorithms with the merits [2].

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2014

Advanced Encryption Standard (AES) and Elliptic Curve Cryptosystems (ECC) is the best two algorithms of symmetric encryption technology and asymmetric encryption technology. This analyzes the AES algorithm and S-box structure, then the replace plan based on S-box structure is proposed to improve AES encryption algorithm, secondly the ECC algorithm is been explained [1]. RSA (Rivest, Shamir and Adleman) is being used as a public key exchange and key agreement tool for many years. Due to large numbers involved in RSA, there is need for more efficient methods in implementation for public key cryptosystems. Elliptic Curve Cryptography (ECC) is based on elliptic curves defined over a finite field [7]. Wireless sensor networks (WSN) are constrained in terms of computational and energy resources. There is enormous research going on for converting the stream based cipher to public key based cipher to increase the level of security in the information transfer in WSN. A recent research validates public key cryptography such as Elliptic Curve Cryptography (ECC) is feasible for wireless sensor network. Also symmetric key algorithms are efficiently implemented and used in wireless sensor network[4].

Protecting the information transmitted over the network is a difficult task and the data security issues become increasingly important. At present, various types of cryptographic algorithms provide high security to information on networks, but there are also has some drawbacks. To improve the strength of these algorithms, we propose a new hybrid cryptographic algorithm in this paper. The algorithm is designed using combination of two symmetric cryptographic techniques [3]. Exchange of private information over a public medium must incorporate a method for data protection against unauthorized access. To enhance the data security against the DPA attack in network communication, a dual field ECC processor supporting all finite field operations is proposed. The ECC processor performs hardware designs in terms of functionality, scalability, performance and power consumption. A unified scheme is introduced to accelerate EC arithmetic functions. The hardware is optimized by a very compact Galois field arithmetic unit with fully pipelined technique [8].

III. AES AND ECC

Cryptography is the study of techniques for secure communication in the presence of third parties. More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and that are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Cryptography prior to the modern age was effectively synonymous with encryption. AES is one among the encryption cryptographic algorithm. Companies usually encrypt their data before transmission to ensure that the data is secure during transmission. The encrypted data is sent over the network and is decrypted by the intended recipient. The encryption algorithms are usually summarized into two popular types: Symmetric key encryption and Asymmetric key encryption.

In Symmetric key encryption, only one key is used to encrypt and decrypt data. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. The key should be distributed before transmission between users. Therefore, key plays an important role in security purposes. Strength of Symmetric key encryption depends on the size of key used. Stream ciphers encrypt the digits (typically bytes) of a message one at a time.Block ciphers take a number of bits and encrypt them as a single unit, padding the plaintext so that it is a multiple of the block size. Blocks of 64 bits have been commonly used. The Advanced Encryption Standard (AES) algorithm approved by NIST uses 128-bit blocks. In the symmetric encryption algorithm we make use of Advanced Encryption Standard (AES). This algorithm supersedes the Data Encryption Standard (DES). AES is based on a design principle known as a substitution-permutation network, combination of both substitution and permutation, and is fast in both software and hardware**.** AES operates on a 4×4 column-major order matrix of bytes, termed the *state*, although some versions of Rijndael have a larger block size and have additional columns in the state. Most AES calculations are done in a special finite field.

Asymmetric key encryption is used to solve the problem of key distribution. In Asymmetric key encryption, private key and public key are used. Public key is used for encryption and private key is used for decryption (E.g. RSA, Digital Signatures and ECC). The term "asymmetric" stems from the use of different keys to perform these opposite functions, each the inverse of the other – as contrasted with conventional cryptography which relies on the same key to perform both. In public key cryptography [4], each user or the device involved in the transmisson have a pair of keys for the

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2014

communication, a public key and a private key and a set of operations associated with the keys to do the operations. Only the intended user/device knows the private key whereas the public key is distributed to all users/devices taking part in the communication. Since the knowledge of public key does not compromise the security of the Algorithms, it can be easily exchanged online. Public-key cryptography finds application in, amongst others, the IT security discipline information security. Information security (IS) is concerned with all aspects of protecting electronic information assets against security threats. Public-key cryptography is used as a method of assuring the confidentiality, authenticity and non-reputability of electronic communications and data storage.

IV. SYSTEM ARCHITECTURE

A.SENDER SIDE:

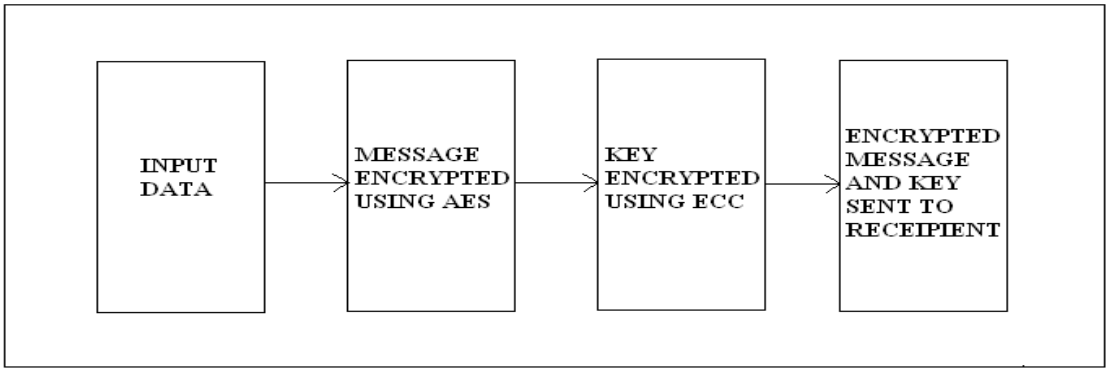

Fig.4.1 System Architecture- Sender side

In this paper, we analyse both the symmetric and asymmetric encryption algorithm. Combining both the algorithm results in the overcome of demerits of one over the other algorithm. Symmetric algorithm being the fast in computation leading to the higher speed in the data/information transmission. This algorithm has issues in the security since there is same key used for both the encryption and decryption. The key exchange should be done in the most secured way for the secured communication. The key exchange is the most important thing to be done in the symmetric algorithm. When there occurs error or defects in the key exchange, then it may lead to the spill of information. In the case of asymmetric algorithm, security is one of the most beneficial parameter which is needed for the network security.

B.RECEIVER SIDE:

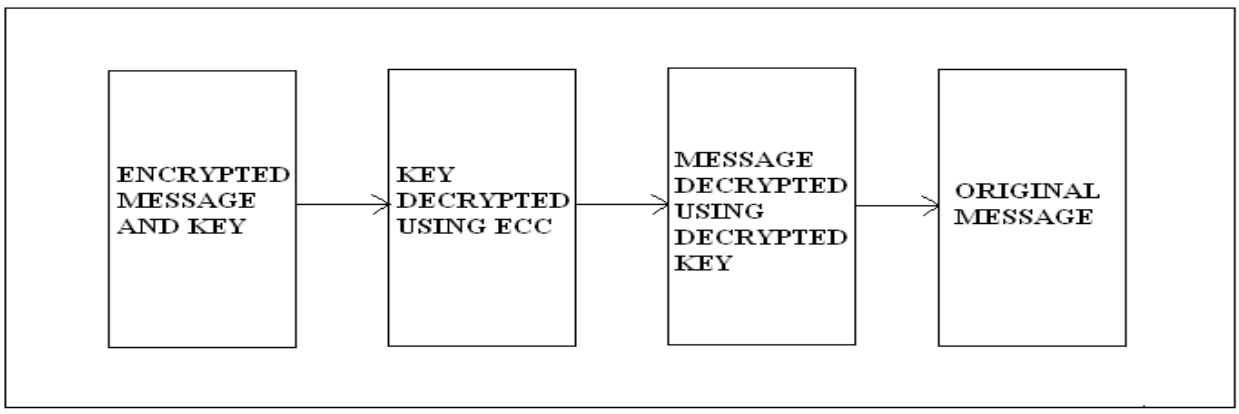

Fig.4.2 System Architecture- Receiver side

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2014

This asymmetric algorithm has two different keys for the encryption and decryption to be done. When there is separate keys then the operation can be done in the most secured way. Public key and private key forms the two different keys for the asymmetric algorithm. This algorithm leads to the time consumption since it needs the separate encryption and decryption to be done in the asymmetric form of algorithm. In order to enhance the security which is predominant role in the network security, we combine the characteristic of both the algorithm. The key used to encrypt the information in the AES is been encrypted using the ECC. The encryption of ECC can be done by means of the public key which is common among the users. This wont be kept secret as the private key. Using the same key the information is being encrypted using the symmetric algorithm AES. As the result of encryption, the text is in the form of Cipher text (unreadable form). The encrypted key which is the public key of the asymmetric algorithm. This key is further decrypted using the private key of asymmetric decryption. Private key is kept in the most secured way to prevent the looting of the information. Private key will be given to the intended user in order to decrypt the message. Then this decrypted key will be given as key to perform the symmetric decryption.

V. ALGORITHM

C. ADVANCED ENCRYPTION STANDARD (AES)

The AES algorithm is done by the series of steps,

1.Subbytes
2.Shiftrows
3.Mixcolumns
4.Addround keys

The SubBytes step:

In the SubBytes step, each byte in the state is replaced with the entry in a fixed 8-bit lookup table, *S*; $b_{ij} = S(a_{ij})$.In the SubBytes step, each byte $a_{i,j}$ in the *state* matrix is replaced with a SubByte $S(a_{i,j})$ using an 8-bit substitution box, the Rijndael S-box. This operation provides the non-linearity in the cipher. The S-box used is derived from the multiplicative inverse over **GF**(2^8), known to have good non-linearity properties. To avoid attacks based on simple algebraic properties, the S-box is constructed by combining the inverse function with an invertible affine transformation. The S-box is also chosen to avoid any fixed points (and so is a derangement), i.e., $S(a_{i,j}) \neq a_{i,j}$, and also any opposite fixed points, i.e., $S(a_{i,j}) \oplus a_{i,j} \neq \mathrm{0xFF}$. While performing the decryption, Inverse SubBytes step is used, which requires first taking the affine transformation and then finding the multiplicative inverse (just reversing the steps used in SubBytes step).

The ShiftRows step:

In the ShiftRows step, bytes in each row of the state are shifted cyclically to the left. The number of places each byte is shifted differs for each row.

The ShiftRows step operates on the rows of the state; it cyclically shifts the bytes in each row by a certain offset. For AES, the first row is left unchanged. Each byte of the second row is shifted one to the left. Similarly, the third and fourth rows are shifted by offsets of two and three respectively. For blocks of sizes 128 bits and 192 bits, the shifting pattern is the same. Row n is shifted left circular by n-1 bytes. In this way, each column of the output state of the ShiftRows step is composed of bytes from each column of the input state. (Rijndael variants with a larger block size have slightly different offsets). For a 256-bit block, the first row is unchanged and the shifting for the second, third and fourth row is 1 byte, 3 bytes and 4 bytes respectively—this change only applies for the Rijndael cipher when used with a 256-bit block, as AES does not use 256-bit blocks. The importance of this step is to avoid the columns being linearly independent, in which case, AES degenerates into four independent block ciphers.

The MixColumns step:

In the MixColumns step, each column of the state is multiplied with a fixed polynomial *c(x)*.

In the MixColumns step, the four bytes of each column of the state are combined using an invertible linear transformation. The MixColumns function takes four bytes as input and outputs four bytes, where each input byte affects all four output bytes. Together with ShiftRows, MixColumns provides diffusion in the cipher.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2014

During this operation, each column is multiplied by a fixed matrix:

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

Matrix multiplication is composed of multiplication and addition of the entries, and here the multiplication operation can be defined as this: multiplication by 1 means no change, multiplication by 2 means shifting to the left, and multiplication by 3 means shifting to the left and then performing XOR with the initial unshifted value. After shifting, a conditional XOR with 0x1B should be performed if the shifted value is larger than 0xFF. (These are special cases of the usual multiplication in **GF**(2^8).) Addition is simply XOR.

In more general sense, each column is treated as a polynomial over **GF**(2^8) and is then multiplied modulo x^4+1 with a fixed polynomial $c(x) = 0x03 \cdot x^3 + x^2 + x + 0x02$. The coefficients are displayed in their hexadecimal equivalent of the binary representation of bit polynomials from **GF**(2)[x]. The MixColumns step can also be viewed as a multiplication by the shown particular MDS matrix in the finite field **GF**(2^8). This process is described further in the article Rijndael mix columns.

The AddRoundKey step:
In the AddRoundKey step, each byte of the state is combined with a byte of the round subkey using the XORoperation (⊕).

In the AddRoundKey step, the subkey is combined with the state. For each round, a subkey is derived from the main keyusing Rijndael's key schedule; each subkey is the same size as the state. The subkey is added by combining each byte of the state with the corresponding byte of the subkey using bitwise XOR.

Optimization of the cipher

On systems with 32-bit or larger words, it is possible to speed up execution of this cipher by combining the SubBytes andShiftRows steps with the MixColumns step by transforming them into a sequence of table lookups. This requires four 256-entry 32-bit tables, and utilizes a total of four kilobytes (4096 bytes) of memory — one kilobyte for each table. A round can then be done with 16 table lookups and 12 32-bit exclusive-or operations, followed by four 32-bit exclusive-or operations in the AddRoundKey step.

If the resulting four-kilobyte table size is too large for a given target platform, the table lookup operation can be performed with a single 256-entry 32-bit (i.e. 1 kilobyte) table by the use of circular rotates.

Using a byte-oriented approach, it is possible to combine the SubBytes, ShiftRows, and MixColumns steps into a single round operation.

D. ECC ALGORITHM

The ECC uses curves whose variables coefficients are finite numbers, there are two families commonly used on the cryptography, the first uses elliptic curves over prime finite field, which is also referred as the odd characteristic or modulo p. It is the field of integers modulo an odd prime number p, where p is large prime number. This one is best suited for software implementations of ECC. The second uses elliptic curves over binary field. This is also referred as the even characteristic or finite field with elements, where m is large integer number. This one is more suitable for hardware implementation of ECC [14]. ()*pE*F *p*F 2()*mE*F2mF2*m*

The mathematical operations of ECC are defined over elliptic curve. For the first type, the elliptic curve is the set of points that satisfies the following equation: , where, such that x, y, a, b. ()*pE*F (,)*xy*23ymod(xaxb) mod p*p*=++324a27b0 +≠*p*∈F
For the second type, elliptic curve is the set of points that satisfies the following equation: 2()*mE*F (,)*xy*
. 2322, 0, where a,b,x,y*myxyxaxbb*+=++≠∈F

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2014

Since all the fastest known algorithms that allow one to solve the ECDLP, need $O(\sqrt{n})$ steps, it follows that the size of the underlying field should be roughly twice the security parameter. For example, for 128-bit security one needs a curve over $\mathbb{F}_q$, where $q \approx 2^{256}$. This can be contrasted with finite-field cryptography which requires[17] 3072-bit public keys and 256-bit private keys, and integer factorization cryptography (e.g., RSA) which requires a 3072-bit value of n, where the private key should be just as large. However the public key may be smaller to accommodate efficient encryption, especially when processing power is limited.

The hardest ECC scheme broken to date had a 112-bit key for the prime field case and a 109-bit key for the binary field case. For the prime field case this was broken in July 2009 using a cluster, it could console, using this cluster when running continuously. The generation of domain parameters is not usually done by each participant since this involves computing the number of points on a curve which is time-consuming and troublesome to implement. As a result several standard bodies published domain parameters of elliptic curves for several common field sizes.

The public key is a point on the elliptic curve and the private key is an arbitrary random number. The steps that underline how ECC algorithm works are described. Figure 5.d.1 depicts the key generation phase.

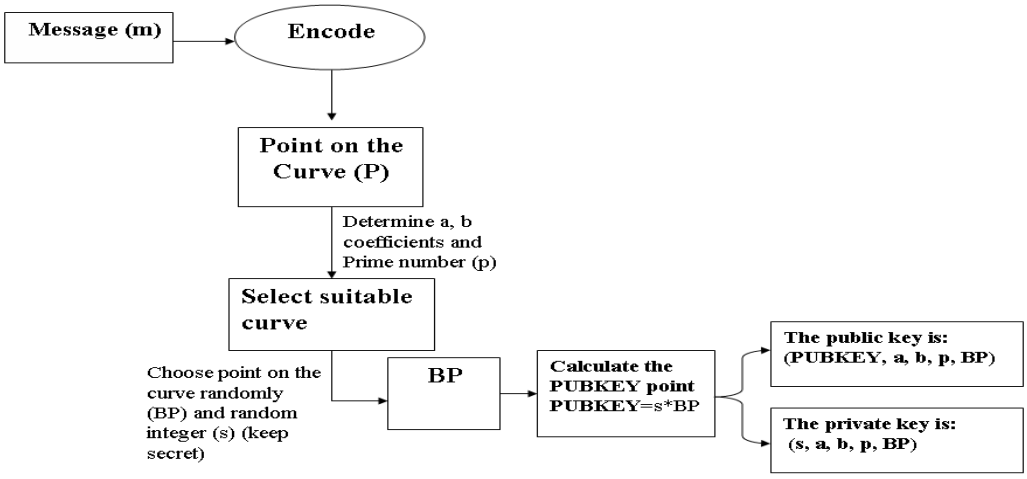

Figure 5.d.1 ECC Key Generation Block Diagram

To encrypt P, a user picks an integer, k, at random and sends the point (k* BP, P + k* PUBKEY). Figure 5.d.2 depicts the encryption operation.

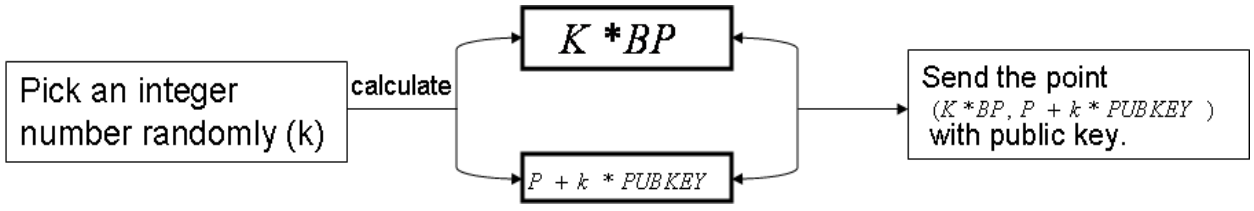

Figure 5.d.2 ECC Encryption Process Block Diagram

Decrypting this message is done by multiplying the first component of the received point by the secretkey, s, and subtract it from the second component, *i.e.*, (P + k * PUBKEY) − s * (k * BP) = P + k *(s* (BP)) − s * (k* BP) = P. This operation is shown in Figure 5.d.3.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2014

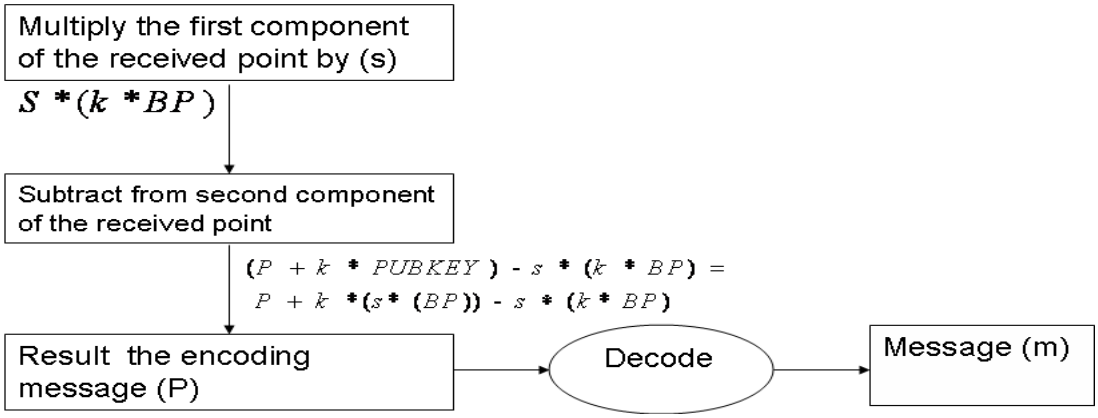

Figure 5.d.3 ECC Decryption Process Block Diagram

VI. CONCLUSION

Secured Data Transfer in using Hybrid Cryptography provides the hybrid cryptography method. For better communication advanced algorithms are used which will be very hard to crack. This architecture provides the secured communication in internet where the speed of the transmission would be high as there is combination of both the symmetric and asymmetric encryption standards. Employing both methods will enable the secured and hish speed data communication. The future recommendations of this project can include the selection of the appropriate encryption algorithms in such a way that all the network resources are utilized effectively and all the resource limitations of the sensor network are satisfied.

REFERENCES

[1] Dinghu Qin, Junli, Wanggen Wan. "Research and Realization based on hybrid encryption algorithm of improved AES and ECC," International Conference on Audio Language and Image Processing, pp.396-400., 2011.

[2] Abdul kader, Diaasalama and MohivHadhoud. "Studying the Effect of Most Common Encryption Algorithms," "International Arab Journal of e-technology," Vol.2. No.1 Jan 2011.

[3] K. Ramesh Babu, Wang Tianfu. "Design of a Hybrid Cryptography Algorithm," "International Journal of Computer Science & Communication Networks," Vol. 2(2), 277-283, 2011.

[4] Jailin.S, Kayalvizhi.R, Vaidehi.V. "Performance Analysis of Hybrid Cryptography for Secured Data Aggregation in Wireless Sensor Networks," "IEEE-International Conference on Recent Trends in Information Technology", June 3-5, 2011.

[5] R. Kumar and A. Anil, "Implementation of Elliptical Curve Cryptography", IJCSI International Journal of Computer Science Issues, vol. 8, Issue 4, no. 2, July (2011).

[6] Eun- Jun Yoon, Kee –Young Yoo, "An Efficient Diffie – Hellman – MAC Key Exchange Scheme" IEEE, Fourth International Conference on Innovative Computing , Information and Control , pp 398 – 400, 2009. Christof Paar, Jan Pelzl, "Introduction to Public-Key Cryptography", Chapter 6 of "Understanding Cryptography, A Textbook for Students and Practitioners". (companion web site contains online cryptography course that covers public-key cryptography), Springer, 2009.

[7] Jerry Krasne, "Using elliptic curve cryptography(ECC) for enhanced embedded security financial advantages of ECC over RSA or Diffie Hellman", Embedded Market Forecasters American Technology International, Inc., November 2004.

[8] Sam Suresh J, Manju Shree.A '' Differential Power analysis (DPA) attack on Dual field ECC processor for Cryptographic Applications'' International conference on Computer Communication and Informatics Jan 2014.

[9] Diaa Salama Abd Elminaam1, Hatem Mohamed Abdual Kader2, and Mohiy Mohamed Hadhoud2," Evaluating The Performance of Symmetric Encryption Algorithms", International Journal of Network Security, Vol.10, No.3, PP.213 219, May 2010.

[10] NeetuSettia.—Cryptanalysis of modern Cryptography Algorithms‖.International Journal of Computer Science and Technology December 2010.

[11] Gurjeevan Singh, Ashwani Kumar Singla,K.S. Sandha, "Through Put Analysis Of Various Encryption Algorithms", IJCST Vol. 2, Issue 3, September 2011.

[12] Monika Agrawal, Pradeep Mishra," A Comparative Survey on Symmetric Key Encryption Techniques", International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05 PP877-882, May 2012.

[13] Mrs. S. Prasanna Ganesan, "An Efficient Protocol For Resource Constrained Platforms Using ECC", International Journal on Computer Science and Engineering Vol.2(1), 89-91, 2009.