POTENTIAL OPERATION OF ELLIPTIC CURVATURE CRYPTOGRAPHY FOR SAFETY IMPROVEMENT

Udhayakumar.A [1] *Ravikumar.K*[2]

ABSTRACT

Now aexistences Elliptic curvature cryptography (ECC) is the most effectual community key encryption scheme based on elliptic curvature ideas that can be used to generate faster, smaller, and effectual cryptographic keys. ECC brands keys completed the posmeetings of the elliptic curvature reckoning in its place of the conservative technique of key generation. This scheme can be used with community key encryption methods, such as RSA, and Diffie-hellman key exchange. Numerical Signature. This newspaper gifts possible use of elliptic curvature cryptography for communiqué network.

Keywords: Elliptic curvature cryptography (ECC), organize system, scalar multiplication, equal of security, Elliptic curve, incomplete field.

I. INTRODUCTION

Quick expansion on electric knowledge safe communiqué in specific is in request for any sympathetic of communiqué network .The chief constituent of safe transportations software stack comprises key conversation and monograms which is obligatory for community key procedures like RSA,DSA and elliptic curvature cryptography[2][3] .Elliptic Curvature (EC) organizations as practical to cryptography were chief future in 1985 self-sufficiently by Neal Koblitz and Winner Miller. The separate logarithm problematic on elliptic curvature collections is supposed to be more problematic than the conforming problematic in the fundamental incomplete arena .Elliptic Curvature Cryptography delivers equal of safety with a 164-bit key that RSA necessitate a 1,024-bit key to achieve, Meanwhile ECC assistances to found corresponding safety with inferior calculating control and battery reserve usage. The ECC concealments all primitives of community key cryptography like numerical sigcountryside,key exchange, key transport ,key group .Currently ECC consumes remained commercially accepted by many regulate group such as NIST ,ISO ,and ANSI [6][7][9].ECC concealments the punishment of arithmetic and processer science and engineering .It can extensively used for electric trade , safe communiqué ,etc. The safety of the Elliptic Curvature Cryptography be contingent on the trouble of discovery the value of k, assumed kpwnow k is a huge Figure and P is aaccidental opinion on the elliptic curve. This is the Elliptic Curvature Separate Logarithmic Problem. The elliptic curvature strictures for cryptographic organizations must be cautiously selected

[1]Research Scholar, Department of Computer science Karpagam University, Coimbatore, India. A.M. JAIN College, Asst Professor, Chennai. umaudhaya83@gmail.com

[2]Assistant Professor, Department of Computer science Karpagam University, Thanjavur-613010, India. ravikasi2001@yahoo.com

NIST(nationwide Group of normal and technology)are creating values and knowledge .

Table 1. Key Scope Forte (Optional by NIST)

[illegible]	[illegible]	[illegible]	[illegible]
104	512	106	5:1
108	768	132	6:1
1011	1024	163	7:1
1020	2043	210	10:1
1078	21000	600	35:1

IV. Presentation Strictures For Elliptic Curvature Curvature Cryprography Application

Even though RSA ,El-gamal and Diffie–Hellman are safe uncorresponding key cryptosystem, their safety originates with a value ,their huge keys. So investigators consume observed for if auxiliary that delivers the similar equal of safety with lesser keys. For Elliptic Curvature Cryptography application subsequent deliberation must encounter :

- Suitability of approaches obtainable for enhancing incomplete arena arithmetic like addition, multiplication, squaring, and inversion.
- Suitability of approaches obtainable for enhancing elliptic curvature arithmetic like opinion addition, opinion doubling, and scalar multiplication.
- Presentation platprocedure like software, hardware, or firmware.
- Limitations of a specific calculating atmospnowe.g., processor speed, storage, cipher size, gate count, control consumption.
- Limitations of a specific transportations atmospnowe.g., bandwidth, answer time.

Competence of ECC is be contingent upon issues such as computational expenses ,key size, bandwidth ,ECC delivers higher-forte per- bit which comprise advanced speeds, inferior control consumption, bandwidth savings, storage efficiencies, and lesser certificates.

V. Presentation Of Elliptic Curvature Cryptography

Many plans are unordinary plans that consume minor and incomplete storage and computational power, for unordinary plans ECC can be practical .

- For wireless communiqué plans like PDA's hypermedia cellular headphones ECC can apply.
- It can be used for safety of Keen cards, wireless device networks, wireless mesh Networks.
- Web servers that need to grip many encryption sessions.
- Any sympathetic presentation wnow safety is needed for our present cryptosystems.

Resultanalysis

In this paper, we have plotted every letters into two arguments on elliptic curve by addition bench. Formerly, we ciphered the consequences arguments by means of a non-singular medium of (2 2). At this juncture, we analysed with present public key procedure to find out our procedure presentation.

-Encryption examination

Our encryption method is very commanding and conventional onward. In this procedure, there are numerous procedures to characterizes an argument on elliptic curve. The procedure is grounded on the (2 2) square medium. Consequently we can choice nonsingular medium noted A with |A|= 1. When associate to other procedure, the RSA procedure computes every and every text adjustable for encryption. The ElGamal procedure products two dissimilar cipher manuscripts for solitary encryption. In our procedure we can brand set of opinions in solitary encryption. The following figure (Fig. 5) clearly designates about encryption approaches of various procedures.

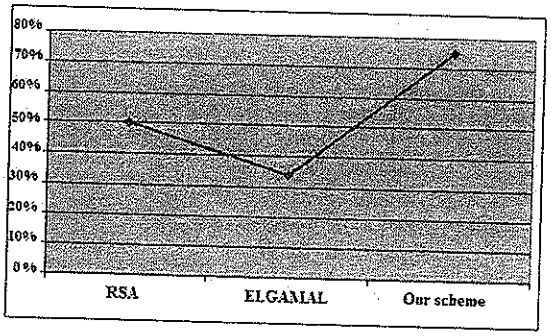

Figure 5 : Comparison performance of Encryption

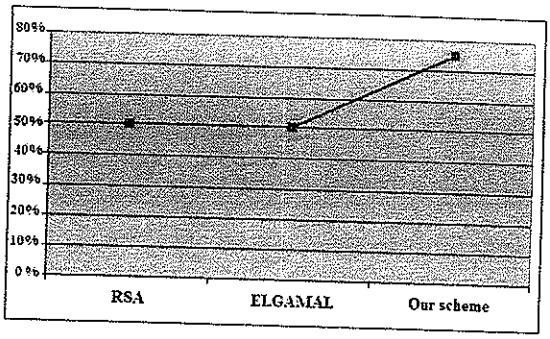

Figure 6 : Comparison performance of Decryption

Decryption examination

Our decryption process is multifaceted deprived of the private key. All the plaintext are decrypted using opposite matrix as a key, So it delivers security from the illegal objects and vulnerable. Likening to other algorithm, the RSA algorithm decrypt the encrypted text one by one. The ElGamal procedure obtains the two cipher text and calculating decryption once. In our algorithm, we receive set of blocks and decrypt in single step. The following Figure (Fig. 6) clearly indicates about decryption methods of various algorithms.

VI. Conclusion

Elliptic Curvature Cryptography suggestions the uppermost strength-per-key-bit of any recognized public-key scheme of chief cohort methods like RSA, Diffie-Hellman. ECC suggestions the similar equal of safety with lesser key sizes, computational control is high. Combined route space is incomplete for keen card, wireless devices.The continuing expansion of values is a very significant location for the use of a cryptosystem. Values assistance to safeguard safety and interoperability of

dissimilar applications of one cryptosystem. Tnow are numerous main governments that grow values like Global Values Group (ISO), American Nationwide Values Group (ANSI), Group of Electrical and Microchip knowledge Engineers (IEEE), Central Increation Dispensation Values (Fips).the most significant for safety in increation knowledge are the in totaling safe communication, Elliptic curvature cryptography (ECC) allowing knowledge for many wireless device networks.

This manuscript presented a technique to surround the communication into the numerous point form and formerly using non-singular matrix for encryption. In the projected method, the same atmosphere of message is planned to dissimilar points by consuming accumulation table of the curve opinions. Consequently, the projected method reinforces the cryptosystem, i.e., for a given intruder it would be very difficult to guess on which points the message characters are mapped and it fleeces letter incidences of the plaintext communication. The test understood on the algorithm showed their sturdiness and their competence. Finally, we like to opinion out that the use of non-singular matrix resolve provide better enactment in this esteem.

References

[1] JeongkyuHong ; Dept. of Comput. Sci., Korea Adv. Inst. of Sci. Technol., Daejeon, South Korea ; Soontae Kim *"ECC string: Flexible ECC management for low-cost error protection of L2 caches"* Published in: Computer Design (ICCD), 2012 IEEE 30th International Conference on Date of Conference: Sept. 30 2012-Oct. 3 2012 Page(s): 512 – 513

[2] Tanakamaru, S. ; Dept. of Electr. Eng. & Inf. Syst., Univ. of Tokyo, Tokyo, Japan ; Esumi, A. ; Ito, M. ; Kai Li more authors *"Post-manufacturing, 17-times acceptable raw bit error rate enhancement, dynamic codeword transition ECC scheme for highly reliable solid-state drives, SSDs"* Published in: Memory Workshop (IMW), 2010 IEEE International Date of Conference:16-19 May 2010 Page(s): 1 – 4

[3] JangwonPark ; Sch. of Electr. Eng., Korea Univ., Seoul, South Korea ;Jongsun Park ; Bhunia, S. *"VL-ECC: Variable Data-Length Error Correction Code for Embedded Memory in DSP Applications"* Published in: Circuits and Systems II: Express Briefs, IEEE Transactions on (Volume:61 , Issue: 2) Date of Publication: Feb. 2014 Page(s): 120 – 124

[4] Paul, S. ; Dept. of Electr. Eng. &Comput. Sci., Case Western Reserve Univ., Cleveland, OH, USA ; Fang Cai ; Xinmiao Zhang ; Bhunia, S. *"Reliability-Driven ECC Allocation for Multiple Bit Error Resilience in Processor Cache"* Published in: Computers, IEEE Transactions on (Volume:60 , Issue: 1) Date of Publication: Jan. 2011 Page(s): 20 – 34

[5] LitingCao ; Beijing Union Univ., Beijing ; JingwenTian ; Nan Wu *"Intelligent Security System Based on Self-Organizing Wireless Sensor Networks"* Published in: Networking, Sensing and

Control, 2008. ICNSC 2008. IEEE International Conference on Date of Conference: 6-8 April 2008 Page(s): 1247 – 1252

[6] Roy, S.S. ; Dept. of Comput. Sci. & Eng., Indian Inst. of Technol., Kharagpur, Kharagpur, India ;Rebeiro, C. ; Mukhopadhyay, D. *"A Parallel Architecture for Koblitz Curve Scalar Multiplications on FPGA Platforms"* Published in: Digital System Design (DSD), 2012 15th Euromicro Conference on Date of Conference: 5-8 Sept. 2012 Page(s): 553 – 559

[7] Bin Yu ; Dept. of Document Examination, China Criminal Police Univ., Shenyang, China *"Establishement of elliptic curve cryptosystem"* Published in: Information Theory and Information Security (ICITIS), 2010 IEEE International Conference on Date of Conference: 17-19 Dec. 2010 Page(s): 1165 – 1167

[8] Schinianakis, D.M. ;Electr. &Comput. Eng. Dept., Univ. of Patras, Patras ;Fournaris, A.P. ; Michail, H.E. ; Kakarountas, A.P. more authors *"An RNS Implementation of an F_p Elliptic Curve Point Multiplier"* Published in: Circuits and Systems I: Regular Papers, IEEE Transactions on (Volume:56 , Issue: 6) Date of Publication: June 2009 Page(s): 1202 – 1213

[9] Janagan, M. ;Arunai Coll. of Eng., Thiruvannamalai, India ; Devanathan, M. *"Area compactness architecture for elliptic curve cryptography"* Published in: Pattern Recognition, Informatics and Medical Engineering (PRIME), 2012 International Conference on Date of Conference: 21-23 March 2012 Page(s): 131 – 134

Authors Biography

Dr.K.Ravikumar, is working in Tamil University, Thanjavur..He has presented papers in 50 International and National Conferences .He is Completed UGC Research Project. He has written 16 DDE Books in Tamil University Thanjavur. He has 12 years Teaching and Research Experience. He is UGC-NET Coaching Co-ordinator for UGC XI Plan .His Research Areas is Network Security, Cryptography, Mobile Computing, and Cloud Computing.r.

A.Udhayakumar, received his B.Sc and M.Sc degree in computer science from the Bharathidasan University in 2003 and 2005 respectively. He received his M.Phil degree in computer science from Alagappa University in the year 2009.He is pursuing his Ph.D research in Karpagam University, Tamil nadu, India, focusing on *"Multiparty Mobile computing security"*. He joined as an Assistant Professor in the Department of computer science, A.M.JAIN College, Meenambakkam, Chennai-114 affiliated to the University of Madras Tamil nadu, India in the year 2005.He is the author/co-author for more than 10 National papers. He is the co-author of *"Elements of Computer Network"*. His papers have received a wide range of awards in the National seminars and conferences. His area of interest is in the field of *networking security.* He had published so for 10 articles in International Journal and obtained **best paper** award for his work on "Mobile Computing Security using Ad Hoc Network".