International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 12 | Dec - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Finite Fields in Numeric and Arithmetic in Cryptography

DR C.P . Indhumathi Asistant prof Bharathidasan Institute of Technology Campus, Anna University, Tiruchirappalli

Prof Pannnerselvam ,Assist prof K. Sathish kumar ,Dr. Dahlia Sam1

Prof Dr MGR Educational and Research Institute Maduravoyal Chennai TN

Prof Dr. Brindha Tirugnanasambandam1 M. A. M school of engineering siruganur Tiruchirapalli

Abstract

Fermat optimal key generation application And that increases data security and privacy security is a major aspect and a fundamental necessity in iot design. This work proposes an approach called optimal key generation using optimization. The encryption technique gives a robust and lightweight encryption mechanism enhances security and efficiency maintaining a high level of security using cryptographic operations making a feasible solution to secure iot networks. Confidentiality is done Using optimal key generation. These techniques are providing sensitive information to provide access to the data making it feasible solution to secure iot networks.

Introduction

IOT has become the smart technologies. IOT interconnects not only internet extranet. IOT spectrum is not limited to connected devices and smart technologies digital payments agriculture and productive Maintenance Smart cities. The review by smart system to be established by 2030 reports that 29.42 billion IOT devices are connected. Also IOT says that there is 16% rise in IOT market in terms of cellular technology which becomes nodal point.

IOT dominently has three modules namely Edge device Gateway and database. A communication is established between the Gateway and database. Edge device handles input such as text image audio video and motion capture. IOT normally gets network has millions of connected entries much more vulnerable to threat injections falsified directions malicious activities while comprising single node. The fundamental requirement is confidentiality as there are confidentiality preservation methods regarding jamming substitution and fiestal structure. There are some Edge devices which have Hardware and battery operated power supply Encryption algorithms are suitable. So we develope lightweight system with less overhead and the power consumed in iot is low.

Avalanche effect

The avalanche is a metric in the framing of crypto system for a small key change produce a different result ensuring avalanche effect. Plain text is normally in all zeros. The proposed encryption system is very sensitive false care no more. It's essential for the hardware analysis. The proposed cryptographic algorithm consumes a max of 1.2 percentage for ciphering Light Weightness of the algorithm in addition to changes of plain text.

The utilization of iot in different applications is an important in technology with strengthens by transformation and data communication. Iot works by the connection of workstations servers and sensing devices and broad variety of iot enabled objects. The large data in iot devices give the security challenges as there is an authorized access and data duplicate. It is necessity and essential to focus on secure communication among gateways of iot in case effective key management system within iot networks.

One of the effective approaches by securing a *IOT* devices.

Proposed methodology

The data communication security is managed through constant data loss. So to build a secure cryptography using iot integrating finite fields in numerical arithmetic optimization with optimal key generation with computational efficiency in terms of encryption time using modern algebra and scalable with adaptive optimization techniques such as cryptographic process and resource constraints without authentication. To explore iot domains and performance enhancement.

To provide robust encryption particularly quantum Computing with cryptographic challenges. Examine a design of iot systems. Also in iot there are in accessible areas and reduced computational demands. Practical research should concentrate in real world iot environment. So we have proposed a practical use and evaluation of Industry iot confined to network simultaneously.

The encryption models constitute data communication loss providing privacy and security thus suggesting an efficient model on data transmission during communication for generating a private key in the encryption process.

Optimal key generation

In cryptography finite fields have become more notable cryptographic algorithms conversions rely on properties of finite Fields. The fundamental elements of a branch of mathematics is groups rings fields known as modern algebra. In a group of finite number of elements it is referred to as finite group of the order of the group is equal to the number of the elements in the group otherwise the group is infinite group.

A field is as a set of axioms. There are two types of fields infinite Fields finite Fields. Infinite Fields not a particular internet in Trend internet in context of cryptography finite Fields are a rule in many cryptographic algorithms.

For a given prime P finite fields of order P, GF(P) is definied as a set ZP of integers {0,1,2,...P-1} together with arithmetic operations modulo p. Recall Here set of Zn of integers {0,1,2,...n-1} together with arithmetic operations modulo n is a commutative ring.

Polynomial arithmetic -Here we introduce a subject of polynomial arithmetic three types of classes are available

I) Ordinary polynomial arithmetic using the basic rules of algebra

II) Polynomial arithematic in which coeffecients performed modulo p , coeffecients are in Zp

III) Polynomial arithematic in which coeffecients are in Zp and the polynomials are defined modulo a polnomial m(x) whose highest power is some integer n

FERMATS THEOREM

The fermats theorem and eulers theorem are in public key crytography

FERMATs theorem states as follows " If p is prime and a is a positive integer not divisible by p then a power(p-1) = 1 mod p

All of the elements Zp , where Zp is the set of integers Zp in sequence ,

Furthur Ax = number mod p

Therefore (p-1)numbers (a mod p , Za mod p ... (p-1)a mod p)}

just the numbers { 1, 2, ... (p-1)}

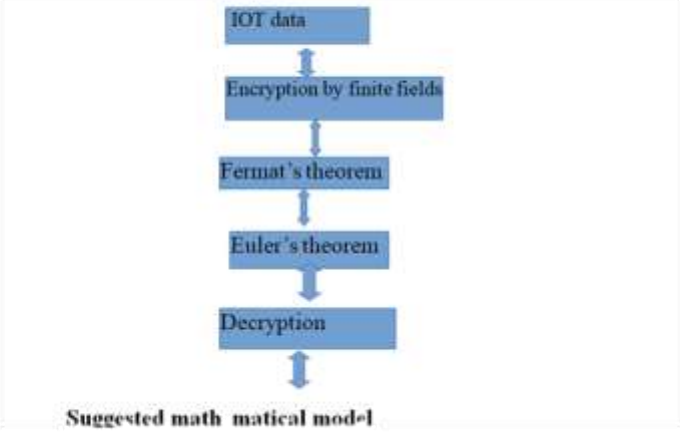
multiply the numbers in both sets and take results mod p yields

ax2ax...x(p-1)a == [(amod p) x (2a modp) x ...x

((p-1) a mod p) mod p == [1x2x...(p-1) mod p]

==(p-1)!mod p

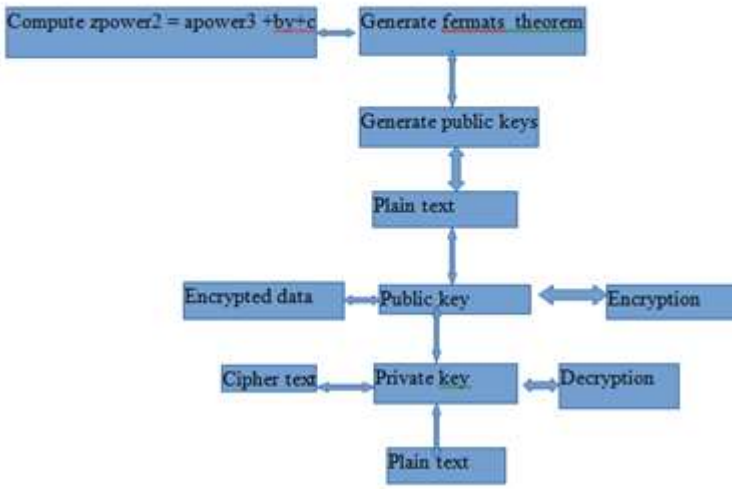
But ax2NX...X((p-1)a) = = (p-1)!a power (p-1)



Suggested math matical model

Suggested mathematical model

Steps in encryption



In an elliptic key cryptography(y,z) is the point
Zpower 2 =a powre 3 + b y + c
a,b are points

Optimal key generation2

The key is utlised for converting plain text to cipher text and vice versa introduced for priovate keyt generation. The encryption process is by randonm number generation. To ensure robustness of the encryption and decryption a new optimization concept is introduced for the positions

Q = Rand 1 < B
X = Rand 2 X I dx + Rand 3 X I dx
Where Rand 1 Rand2 and Rand3 are vectors generated randomly
in the range of [0,1]

It is computed a mean position of a a is given as follows :

a = 1 / x z i
A distance is computed on elliptic coefficients on polynomial arithematic as given

E d (i) = (summation j = 1 to d (y i , j - U j))

In each iteration , a farthest from U leads the algorithm. The computational stability and efficiency has certain challenge . During the initial phase the loss of diversity in the optimized solution.
Second the predator has a high speed of encrytpion and decryption making it hard. So two enhancements are capable.

Convergence enhancement
An enhancement to improve the rate of convergence is the initial stages of optimization several elite are chosen to compute. This should decrease or increase the computation.

It is given as

m(t) = [M min / 1+ (M min / Mmax)]

This is the key generation process and enhancement where Encrytpion time for encryptiing the data is ET = Encrypting total no of bits
Encryption rate

E T = Encrypted total no of bits
Decryption rate

Encryption time ---> Time taken for encrypting given data suggested by the algorithm

Key generation time ----> Time taken for generation suggested by the algorithm

Conclusion

The industry experiences Users to detect actual environment into a conventional development that transforms realistic physics so that the focus is on building detection scanning for product lines exploring developing a code to decode from the given plain text to Ciphertext. The suggested model addresses the need for high level of security the Practical implications in iot settings are significant and compass various iot researchers iot networks comprise safe communication Improvement especially in smart cities or industrial iot networks. Here The Matrix provide a quantitative way to assess the quality of internal product attributes thereby enabling a firmware engineer to assess quality Double pervasive constant consistent and objective.

Future work: Geometry symmetric key cryptosystem consumes significantly less powre consumption in intel. This involves a single round of sufficient probability characteristics

References

[1] Cryptography in IOT using elliptic curve cryptography with adaptive hunter pray optimization C. A. Yogaraja, R. S. Sankarasunramanian M. Geetha and R. Keertanadevi

[2] An intrusion Detection System in WSN using an optimized self - attention based progressive Generative Asversarial based progressive

R. Saravana Ram and A. Gopi saminathan

[3] Design and analysis of high speed phase frequency Detector with zero zone in PLL peta Guruprakash kumar and Darshak Bhatt

[4] Spectral pyramid pooling and fused key point generation in Reset-50 for robust 3 D object detection

V. Vasudevan and B. S. Murugan

[5] A new Low-power Hybrid Full Adder using CCGDI technique for a portable MAC unit Biswarp Mukerjee

[6] Block chain based electronic health record system R. NagaPriyadarshni Bhawana tyagi B. R. Harshath and R. Vinoth kannan

Dr C.P Indhumathi Assistant prof (Sr grade) is working as Asistant prof (Sr grade) Bharathidasan Institute of Technology Campus, Anna University, Tiruchirappalli has Research Area in Software Engineering, Software Testing, Optimization Techniques , Object Oriented Design Patterns , UI/UX Design Concepts Software Defined Network is having 15 years of experience

Authors Dr T.Brindha is currently in an Associate professor in M.A.M School of Engineering for Computer Science Department, Artificial Intelligence and Data Science, Trichy, Tamil Nadu, INDIA. Her interested areas include Data Base and Management Systems, Computer Networks, Object Oriented Analysis and Design, Artificial Intelligence, Big-Data, Cloud Computing, Python, Bio-informatics.

Dr. Dahlia Sam is currently working as a professor at Dr. MGR Educational and Research Institute Dr. Dahlia Sam received her PhD degree in Nov 2016 from Dr. M.G.R. Educational and Research Institute, Deemed tobe University, Chennai, India. She has working experience in Research Institute. She has published many papers in reputed journals including Elsevier, holds an Indian Patent, an Australian Patent and was selected for Women's Scientist Scheme WOS-C. She has 6 research scholars working under her supervision. Her main research interests include Vehicular Networks, Machine Learning, Artificial Intelligence and Neural Network

Pannerselvam is a professor and K. Sathish kumar is a Associate professor in M.A.M school of engineering