TEST Engineering & Management

January - February 2020
ISSN: 0193-4120 Page No. 16907 - 16916

Experimental Analysis of Finite Field Over Prime Field and Binary Field

Dr.Sonali Nimbhorkar[1], Dr.Swapnili Karmore[2]

[1]Computer Science & Engineeering, S. B. Jain Institute of Technology, Management and Research

Article Info
Volume 82
Page Number: 16907 - 16916
Publication Issue:
January - February 2020

Article History
Article Received*: 18 May 2019*
Revised*: 14 July 2019*
Accepted*: 22 December 2019*
Publication*: 29 February 2020*

Abstract

As new-fangled attacks come up, protocols desires to be verified all over again and also require cultivating some new arise protocols that can resist the different kind of attacks. A secure system is dependent on the use of cryptographic techniques. Potential use of finite field for the implementation of elliptic curve cryptography which is supporting to implement and design the different key establishment protocol such as key agreement,key exchange protocol that are vulnerable to various kind of attacks (active and passive attack).Finite field accomplishment improves the confidentiality and efficacy of communication network .Finite field arithmetic is used to provide efficient and secure elements for cryptography for key establishment and key exchange . The major emphasis of this paper is on appropriate implementation finite field operation over prime field(Fp) and binary field(F2m).

Keywords; *Elliptic curve cryptography, finite field, binary field prime field ,scalar multiplication, point addition, point multiplication*

I. INTRODUCTION

The geometric representation of elliptic curves over finite field is main sub-division of ECC arithmetic. Elliptic curves (EC) over finite field are simple geometric tasks, which can be illustrated as gradually encompassing outlines provided in the plane (x-coordinate, y-co-ordinate). Since 20th century mathematician concepts of elliptic curve theory studied and produced some significant results. Victor Miller and Neal Koblitz have, separately, projected using elliptic curve in cryptography in 1985 [13]. In the past years, using elliptic curves (EC)in cryptography has become more and more popular. They are mainly used in coding theory, pseudorandom bit generation and number theory [12]. An Elliptic Curve over finite field of order n represented by E(F) can be distinct by the long and generalized weierstrass formula equation[5][7]. ECC is based on Diophantine form equation of elliptic curve which is based on usage of number theory. Elliptic curves over finite field can also offer varieties of public-key systems that are quicker and practices to makes use of smaller keys, while on the condition that only on the comparable level of security. The main benefit of diverse kind of calculated group for public-key based mathematics that altogether useful for real-time implementation based public-key systems use properties of arithmetic by means of vast finite groups.

An elliptic curve established on Galois Field is precisely determined by abbreviated formula that is represented by two form with 2 variables and 3 variables, and with their respective coefficients. In cryptography, the procedure for selecting proper variables and quantities are limited to features defined using Galois or finite field, which outcomes in determinant of abelian group laws which is a conventional series of elements through performing arithmetic processes on those elements. The concept of group in elliptic curve, such defined specific operations is performed geometrically. Familiarizing more with desirable attributes and features of a group, such as controlling the quantity of points generation on such a algebraic structure, which

Published by: The Mattingley Publishing Co., Inc.

January - February 2020
ISSN: 0193-4120 Page No. 16907 - 16916

further generates an essentials of finite field on elliptic curve group [1-11].

II.LITERATURE REVIEW

The main concern in security is how to achieve the competent and deployable network for any trustworthy purpose for military and rescuer areas. In relation to security aspect, there are various mechanisms those are needed to be preserved such as data integrity, confidentiality, authentication and denial of service. Concealment continues that the only specific communication is to be acknowledged by the authorized and approved receiver party [7] [8]. Key Management in ECC for Protocol Model using Public Key Infrastructure which focuses on what way to resolve the security concerned issues of ECC and protocol for Key management amongst user and server authority and system for Key Management (KM). The adjustment and enhancement is a innovative methodology that regulates key based operation using ECC among server Authority and Key Management System [12][13].Numerous improvement was suggested with Diffie-Hellman key exchange. The anticipated protocol consumes an implicit asking protocol which is efficient for RSA based secret calculation. The organization of the anticipated protocol system also impervious to all categories of active and passive attacks. Well known passive attack violates efficiency which is not suitable for recommended protocol, so that the effectiveness of the existing protocol is not surrendered. When the complexity is used as the parameter for determining the level of required security is determined then exhaustive search to be carried out up to 2112, the anticipated procedure can accomplish protocol of Diffie-Hellman key exchange using modular multiplications for 108 times[22] [23]. Various public-key cryptosystem based algorithm are available such as RSA, ECC and DSA. Nevertheless Elliptic curve cryptography is different as of RSA, Due its faster growing capacity and effectivity and another way for researchers to makes use of cryptographic algorithm. As the security level achieved by RSA, that ECC can be delivered with lesser number of keys as illustration, the 1024 bit security strength provided by RSA that could be provided by ECC using 163 bit security strength. Further, ECC is principally well-matched for devices intended for wireless communications, such as mobile phones, smart cards and PDA's. Process of point multiplication operation using elliptic curve is initiated to be computationally effective than process of exponentiation in RSA [27][24]. The most important parameters are utilized to define efficacy that are cost in encryption is due to the computation, the amount of operations depends on the addition chain used[12][14][18].

II. DOMAIN PARAMETER GENERATION

Parameters of elliptic curve is defined on the finite field such as F(p) or F(2m) can be termed by the set of tuple .At a distance from parameters defined by curve by means of elements a and b, and there are other parameters that must be established by intended parties which are involved in protected and confidential communication using Elliptic Curve structure.

A. Domain Parameters for Elliptic Curve over Prime Field

The realm parameters used in support of Elliptic curve (EC) defined over prime field or F(p) are p, a, b, Gx, Gy, hand n, anywhere p is the prime number defined for finite field F(p) and a, b are the essential parameters are significant on the defined curve y2 mod p= x3 + ax + b mod p. Also generator G is the random generator point (xG, yG), is a random point on the elliptic curve preferred for cryptographic operation, where n is the order of the elliptic curve. The scalar for point reproduction is chosen as a number series between 0 and n – 1. Cofactor (h) is universally h = number of points E(Fp)/n on an elliptic curve[13][15][17].

Published by: The Mattingley Publishing Co., Inc.

January - February 2020
ISSN: 0193-4120 Page No. 16907 - 16916

B.Domain Parameters for Elliptic Curve over Binary Field

Implementation consideration of NIST and SECG suggested and recommended for binary field and generic curves completed on key sizes ranging from GF(2^{163} ,2^{233},2^{283}, 2^{409},2^{571}) [7][11] are considered. In comparison, if the curve is defined over a binary field, the set of parameters is P= (m, f(x), a, b,G, n, h), where m is the positive digit of bits that specifies the field GF(2m).

• Polynomial f(x) is of degree m. where F(x) is irreducible polynomial.

• Parameters a and b are describe on the defined curve E for F(2^m).

For implementations of a miniature number of fields $GF(2^m)$ with provided irreducible polynomial in-terms of {M1,M2,……..,Mr}. It is a realistic explanation to add committed reduction logic for each F(x) i.e. Irreducible polynomial. The discrete logarithm problem on elliptic curve groups is believed to be more difficult than the conforming problem in (the multiplicative group of nonzero elements of) the underlying finite field based on characteristics of 2 or 3 are characteristics equation in binary field are follows [6] [17][28][49].

III. CATEGORIES OF PERFORMACE EVALUATION OF FINITE FIELD

ECC calculation in Galois (finite) Fields is crucial element of numerous asymmetric key encryption based procedures, comprising entities constructed on the obstruction of DLP (problem of discrete logarithm) in presentation of finite fields and mathematical schemes used for elliptic curve operation. The accomplishment of such arithmetic schemes determined on the basis of execution of the arithmetic in the primary use of finite field. The figure 1 demonstrates the Different classes of finite fields that are offered in asymmetric key encryption scheme; these types of finite field were concisely designated in figure 1.

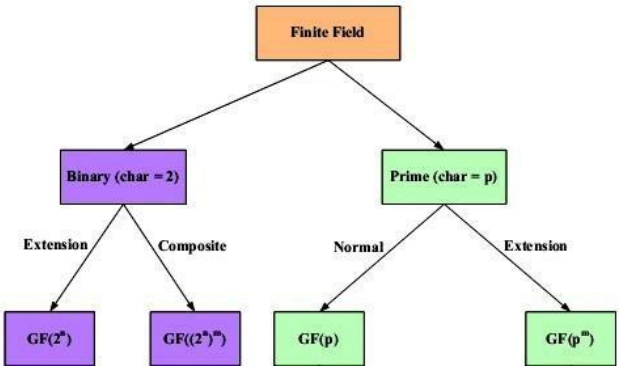

Figure 1. Categories of Finite Field GF

A. Performance Requirement of Prime Field

The operation on the prime field GF (p) for big prime number p along with field order is challenging for usual computers and having calculation difficulties. Numerous machine words are necessary to characterize features of this field; meanwhile usual machine word sizes are basically not sufficient. The main issue with demonstration is that throughout the process of computation, it carries between words must be broadcasted, and also performed operation of reduction modulo of p on numerous machine words.

There has been a huge volume of investigation deals with approaches for undertaking elongated-number and multi-precision mathematics proficiently; the main accepted method in this perspective which is based on the reduction of Montgomery. On the other side, using the processor's multi-precision arithmetic demands cost to time efficacy, particularly with the operation of reduction modulo of p[1][3].

B. Performance Requirement of Binary Field

The binary field GF(2m) is a widely used for hardware circuit design using finite field multipliers, which characterize the features of the field GF(2) using rational values between “0’s" and “1’s”. Operation of binary field involves m number bit-wise actions which make use of irreducible polynomial; this also leads to marks field operation simple and added proficient. Nevertheless, such type of field doesn’t compromise the similar computational benefits in a software execution,

Published by: The Mattingley Publishing Co., Inc.

January - February 2020
ISSN: 0193-4120 Page No. 16907 - 16916

subsequently its amore advantageous in hardware by using simple XOR gates in contemporary microprocessors that are designed to be proficient for actions that transaction more with huge bits; in this cases, it creates the procedures which are slow for large values of m bits [12][15][17] .

IV. TECHNIQUES OF SCALAR MULTIPLICATION

The most time consuming accomplishment using ECC is scalar (point) multiplication or scalar multiplication. For speeding up this process, numerous approaches, methods, and algorithms exist, like choice of an basis for finite field which is suitable for secure implementation in hardware and in software based on selection of a representation of the underlying finite field. The purpose is to select such representation, which provides the fastest arithmetic in the field. This is possible due to the existence of some representations of finite fields that have computational advantages over the other representations, selection of an elliptic curve[14][15][16].The point scalar multiplication is attained by repetitive processes of point addition (PA) and point doubling (PD) actions. The most important cryptographic setup of ECC is attainment of scalar point multiplication which can be calculated using computation Q = k*P, where point P is multiplied via an integer k resulting in a more resultant point Q on the defined curve.

Intended for the accomplishment of point scalar multiplication subsequent methods are used [2][3][24][27]:

- L-T-R (Left-to-right binary) Scheme
- R-T-L (Right-to-left binary) Scheme
- NAF (Non-Adjacent) Form
- W-NAF (Width w Non-adjacent) Method
- Method of Joint Sparse
- Method of Double and Add
- Method of Addition Chains
- Method of Fibonacci and Add
- Montgomery Method

Algorithm for scalar multiplication	Time complexity
Right to left binary method	Approximate average running time complexity is:-(d-1/2)A+(d-1)D
Left to right binary method	Approximate average running time complexity is (d-1/2)A+(d-1)
Width- Non-adjacent form	Approximate average running time complexity is :-(D + $(2^{w-2}-1)$A) +((d/w + 1-1)A + (d − 1)D)
Joint Sparse Form	[k]P + [l]Q
Addition Chains	aA+(s-a)D
Fibonacci and Add	O(n log n)
Montgomery method (Ladder)	$x^{-1}2^n \bmod N$

Table I. Time complexity of scalar multiplication schemes

In table I shows the analysis of time complexity of various algorithms used for scalar multiplication.

V. ECC IMPLEMENTATION ISSUES AND CONSIDERATION

Cryptosystem implementation enforces several Challenges, which may require a swapping in accurate presentation, security and flexibility. Elliptic curve cryptography (ECC) can be executed in software implementation and hardware implementation. Software implementation in Elliptic Curve Cryptography offers reasonable speed and higher power consumption compared to conventional hardware. Additionally, software implementations have exceptionally restricted to physical security, specifically with values of key storage.

The environment used to run the tests and also present the consequences of implementation and execution in java, processor Pentium IV Dual-Core CPU T6670, 2.20 GHz , Linux operating system[11][12][13].

To make use of ECC primitives, all intended parties must be in agreement on every essential element on the domain parameters for elliptic curve implementation. The accomplishment of finite field

Published by: The Mattingley Publishing Co., Inc.

TEST Engineering & Management

January - February 2020
ISSN: 0193-4120 Page No. 16907 - 16916

GF(p) for huge prime number (p) on usual machine is also have calculation and communication complications. Several computer needs number of bits (words) which are necessary to characterize basics of finite field, subsequently distinctive word sizes are not large enough. The main difficulty through demonstration is that throughout calculation and execution, which carries number of bits must be broadcasted, and the operation of reduction modulo p must be designed over a number of Bits [8][12][14].

VI. FINITE FIELD IMPLEMENTATION

There are numerous choices that need to be prepared before implementing an elliptic curve (EC) based system. Among them is the elliptic curve underlying field and field representation is used to implement ECC based cryptosystem. In this segment characterize the purpose finite fields and show that the points on elliptic curves satisfy the properties of finite fields. A finite field includes a finite set of elements collectively with four binary operations called addition, subtraction, multiplication & division which convince certain arithmetic properties. The security of ECC lies on the difficulty of elliptic curve discrete logarithm problem. The main operations involved in ECC are point addition, point doubling, point multiplication.

A. Prime field Implementation

The Elliptic curve domain parameters defined over prime field F(p) are p, a, b, gx, gy, n and h, where p is the prime number defined for finite field F(p) and a, b are the basic parameters significant on the curve. Weierstrass Equations Depending on the characteristic of the field K, the equation can be significantly simplified Characteristic p: with p (2,3), fields Fp[3].

	A	B	P	Order	Generator X	Generator Y	Private key	Public Key
16Bits	44514	1296	52999	79847	79847	40788	18166	X=45225 Y=8259
32 Bits	504179098	221354884	4059007387	6204621847	3378586977	3797126563	154360401	X=1172498229 Y=1812602312
64 Bits	5864143036732783513	8280848717103568225	17604934993366634743	28586196868155734791	2183150467594410852	1161969371278573250	16794647628515612364	X=15837142834028551599 Y=4989682548876214112
128 Bits	41967051046836267087380291859339694567	38268281057957801407997115194480598025	241823592279649851285752638348442085407	519008473195980192888324457010931412439	183917942963791913970272355858802850594	7598110471179209335208315111622558609	7598110471179209335208315111622558609	X=136055464568248114888296010778308180057 Y=144019322880467894977233127903680515341
160 Bits	297190522446607939568481567949428902921613329152	173245649450172891208247283053495198538671808088	1332297598440044874827085558802491743757193798159	1332297598440044874827085038830181364212942568457	1089473557631435284577962539738532515920566082499	127912481829969033206777085249718746721365418785	395136021986583482292509064076039706863304530823	X=1059936952642611106927116654212865258744120714969 Y=366010833437214675828209994085179043066446894728
192 Bits	2613009377683017747869391908421543348309181741502784219375	1731160591135112004210203499537764623771657619977468323273	47816689839061662429550018943449237732591196552530131933 67	47816689839061662429550018942690383081198636591198348689 29	47231888565143929353993376991535221735251686210813416816 22	50788478310138774174974695020906110157975525580965213684 7	61867928421865174368662529198075025220840261446368162469 23	X=1341849052296214349836541219486242748445138741708686790797 Y=1826306349784563907921251327467874253179908534808814497915
224 Bits	11020725272625742361946480833014344015343456918668456061589001510723	394960662605337403078792645769513976611844294605231	2272162293245435278755253799591092807334073214594499230443547294131 1	2272162293245435278755253799591092361256754634233075719139656096655 9	14283649272442017264314982074754864969930672673185208441374487839 97	93375553604488232278124107531774686312155587790205180847526188162 05	21107637609049439590975406217105228445545296675651284564163646982 12	X=10177699643897501355475128151691194587872583362025990144332496311814 Y=209972654161943629362216593

TEST Engineering & Management

January - February 2020
ISSN: 0193-4120 Page No. 16907 - 16916

	A	B	P	Order	Generator X	Generator Y	Private key	Public Key
		141151352895898 7						837266662828532726862275321183536093 56919

Table II. Domain parameters generation and key generation based domain parameters in F(p).

BITS	Sender's		Receiver's		Shared key
	Secret key	Public key	Secret key	Public key	
128	73363395 70165574 58896653 93371994 027151	X=9098739 629762462 979620178 551415649 38 Y=1897786 330180311 219054861 853981792 58643	19203264214 71406323065 39121383225 428488	X=1735050 030772203 565704631 187174305 50342 Y=5874667 491325188 822929126 738404252 7079	X=1911768 493972230 008362599 423051011 63621 Y=6342679 341019325 947082205 139795729 0298
192	55151236 51627866 62942433 13457624 91747485 46523516 35089982 82	X=1849817 095424006 622062537 259616773 026426032 457284058 339611 Y=2273469 817102800 936893796 179590371 326708222 163257031 486468	56700087082 66090058146 35716272557 82579728990 90813777407 754	X=8290940 362872923 528239462 601169012 147767287 484923502 90841 Y=1897647 322730395 964543740 201728074 238818121 600374900 391590	X=3461026 454823160 752469370 632993657 067338555 909433950 347717 Y=3933225 691615379 461556938 636710901 409749987 326749669 385336
224	77843028 15737314 05719987 75448066 16649749 77739671 15384610 72462541 0	X=2112686 422244608 955112519 696303800 896092749 630956397 250370439 0450594 Y=1211543 800341309 400747755 701053557 622170759 756412562 082459781 4228195	24713121752 41026516734 90053758213 12783754016 09312222045 91359318362 89	X=1538151 557007198 132701516 275607808 917952427 453804122 198498543 2666087 Y=1283324 399492742 072864629 240867026 085261184 266124809 701235257 6124646	X=2218338 144585565 832012839 181716077 745326055 984587033 033069676 126284 Y=1684316 103594919 707469630 704388817 593449611 393210161 883375664 2363051
256	62913212 23908355 44380146 00093834 61331456 55290825 64043030 19580282 55876997 42248	X=6121765 381435409 268733779 701271423 413064545 606750166 025157343 824009318 2275336 Y=7569468 188724496 432984503 231074636 786793098 539056791 628194119 447303170 5236117	16399813345 94089154363 92050771973 07626848593 48511900921 39365422960 84180961071	X=6428002 251813015 396159257 710778642 350489850 389796789 847449639 189032515 8358635 Y=1590600 638779422 630082957 267400174 351434423 658166459 598958592 284613642 063450	X=1438374 407057386 705727855 498915891 736003730 341670052 086944572 591281246 2108061 Y=7280764 448887888 337250438 447222748 218810836 167412965 801093057 752356029 5630669

BITS	Sender's		Receiver's		Shared key
	Secret key	Public key	Secret key	Public key	
384	35587258 11477393 81656164 31836728 26314610 62150563 73483333 66290198 33850072 81479653 73149465 21189651 28061584 19062495 1826	X=1699929 300487446 599939259 583910503 351165094 577864109 319200326 443942933 159735148 976402350 963713685 910174015 437715599 8 Y=6507061 106226728 398471822 442692579 304146897 357653749 739939364 118751315 172208884 300320058 032087560 163956746 977166641	11239044167 41773043827 05936562087 16112573412 89658443115 96249374222 48683343469 16668087228 88384199499 05895208966 122215	X=1664809 068613197 273166823 356371477 478906481 621734590 163123806 969399940 283946784 571523385 151267555 081246600 753809147 Y=9211468 410362294 331149363 579228797 036406164 441256200 495713404 351643547 493558850 843441666 920096549 114373276 811380588	X=5156182 681087815 466283903 856640215 307158369 248952558 895280197 487645529 078484814 746525201 058161126 955652017 237839396 Y=3028644 943366288 547362463 157846220 710838951 671442988 815125615 131916767 096751272 211910748 787744478 900118620 646819424
521	37861439 53370954 21524323 90957903 91048563 64146355 46400669 38381889 39404214 64156022 31018017 50659679 61778630 72849991 62465884 46079017 90853400 64393723 06616457 08233	X=4661938 405445796 840279751 578419427 684349263 584143953 780188898 397702313 183511679 475528047 752459623 753928678 282881218 571949476 188008420 680688441 945772960 888217 Y=5095365 926300800 131621701 489515217 591676079 590920016 091768441 854080621 953856837 485554169 606890709 677206693 167538918 162019526 278545487 379070272 276235889 495025	39999834074 63788395102 84510386253 58508819128 69862481718 86850419578 09295191507 13331401933 38847634641 49545270863 13122192922 40886632532 91323696018 13967953709 176	X=3040404 438412352 811487374 966342253 140303522 076376443 297242047 668659735 923947852 075818715 309391658 413715457 961396076 727714745 744979867 867257711 049081361 583757 Y=5437021 852357624 555217991 907068834 647892014 901279666 049529407 671479914 644510598 445406575 639691145 817736608 130360738 623571433 656528967 730541378 960788902 285465	X=1523274 212763292 675145990 013069136 786572975 636935217 366094540 175998315 565487436 917406384 086062660 126011972 213756164 254727196 736390650 589221166 184701445 93458 Y=2524479 739738488 098234882 589519479 026699632 531448413 125840144 455490210 141643189 358714242 585979470 922026346 244831934 006491658 498094752 868225122 470448252 564939

Table III. Generation of shared key for Prime Field GF(p)

B. Binary Field Implementation

In Binary field , implementation consideration of NIST and SECG suggested and recommended for binary field and generic curves over GF(2^{163}), GF(2^{233}), GF(2^{283}), GF(2^{409}), GF(2^{571}) [7][11] are

Published by: The Mattingley Publishing Co., Inc.

January - February 2020
ISSN: 0193-4120 Page No. 16907 - 16916

considered .In comparison, if the curve is defined over a binary field, the set of parameters is P= (m, f(x), a, b,G, n, h), where m is the positive integer that specifies the field F2m.

No. of Bits	B	Fx	Generator X	Generator Y	Private key	Public Key
163	29822362 34343851 33626744 66566277 85008148 01587558 1	1169201 3098647 2233456 2947866 1730264 1572474 6034400 9	57599 17430 71675 39422 28907 52155 68343 09477 85672 2486	12167227 71297916 78623892 86186593 24865903 14808241 7	3251671 6356598 4526425 7862485 6792275 6825025 9883957	X=84878100 14833815018 29712851735 58674896549 38143091 Y=86943908 86467270715 60968549336 11804333442 27208548
223	27604979 80029204 18707884 55023778 98520307 70725625 90039643 98570147 123373	1380349 2693581 1275748 6951172 4554050 9049022 1794435 9662576 2565270 2845337 7	67612 46501 58340 90839 97096 88215 98240 46681 24646 58124 68867 44464 34420 21771	69129130 04411390 93209488 94119045 87007871 50872395 12935645 67204383 952978	9825522 4162027 8046207 8593589 3343225 1003212 1825380 1638398 9653047 8255945	X=58136900 54161596357 46228164191 93999370527 55983019369 13941247623 3602325 Y=10395008 34880069774 63736007522 33842616406 10379584802 93260105385 49283412
283	48218135 76056072 37400699 77803990 81180312 27003030 06012701 20450341 20591464 43786169 63829	1554135 1137805 8325673 5569525 4588151 2531392 5471241 7116170 0144992 7791123 4281641 6679896 65GeneratorX=1 1604587 4874070 0369988 2500449 1775374 6571978 4002620 0282129 8087129 1231978 6030478 7296264 3	11604 58748 74070 03699 88250 04491 77537 46571 97840 02620 02821 29808 71291 23197 86030 47872 96264 3	66127200 53854191 97841260 93575635 45875491 15318850 19063529 80899759 34527517 04526244 46196	2153828 5877685 7089371 5697407 1755306 6324803 3469323 3600927 4386872 2958719 0533046 6205655 2	Key X= 44023767062 31220794612 18790319339 10843753775 65927651474 68793973784 75875964077 41292629 Y=10454641 26285437419 22048253239 86157381650 95671936465 90401348941 51468926157 70174966069 1
409	86886261 63409070 76728177 70640384 42526450 58294790 43641824 43865861 41118704 71004564 98863441 08090582 07142318 57121214 79358925 75	1322111 9375804 9719790 3830616 0655420 7965680 9365928 5624385 6929759 0548811 5824726 2269165 0378420 8794307 2443768 7334722 5810789 99041	90193 52799 19555 46051 99380 20229 62770 44091 49556 25144 19635 87868 71544 05187 97594 85130 02772 60702 07382 87319 83206 45356 77571 35484 583	25227180 44786639 65520986 39889290 82234860 48997352 74372668 70837698 58460083 13423032 41905078 14191768 19198459 37270836 69152319 238	9607883 7176030 7824997 1300728 8584412 0281781 9958461 4629983 6385465 4170964 5611336 7043359 4442303 1062432 2072416 3614679 6075700 9601	X= 12692332411 57732104327 04479891709 92009189568 88287607746 73261048355 94182837028 05292731426 32067993036 05356465462 16926752619 247 Y=73425719 52448352496 53676788548 91067025554 73461764023 62856236453 18545250508 18060530022 86379991064 73422493544 56961148310 77089
571	28533292 45261343 53556008 69641815 51296889 29877610 68329808 91560850 94418001 17011233 07905326 01964265 26535330 03482753 02366901 68428841 08172514 87094414 06111136 79225347 41972021 7210	7729075 0460345 1668939 0703781 8639746 8859785 4659412 8699973 1447050 2903038 2845791 2084907 2387533 1638451 5592492 7232063 0043543 5473015 7322085 9753114 8581734 6934161 4973939 6162964 7909	29097 26711 39336 02389 97027 32507 99810 94903 29308 34162 77207 16319 15331 86952 17984 69486 91035 43565 12732 52692 73106 04572 49729 60551 31292 33502 61550 70992 13961 91312 12148 31097 56525 47904 25	33661747 31810125 75308781 32097086 76894833 15035859 57787521 45226712 85810278 36122776 07950241 45209019 25250058 83890170 63917460 51503941 68627448 70712681 18484551 02037101 82566571 2475	5358728 1374825 4091014 6655344 4318758 7650782 9710386 5330445 2190075 2096498 9619594 8277318 2825779 7520688 4912323 3728184 9437830 1300003 9361704 6385699 5550062 9462547 8730320 9648704 7659	X=45226333 25866583900 53551322460 06813551966 54302226507 18723782585 34934931044 39209669680 88839473028 26126716385 24982357026 99789945903 52309829114 15436793477 97908233135 6148229974 Y=42794994 66704363082 73552726063 44311467307 22093688559 22329963218 59495669279 76067469614 68772041472 09316105887 41400739442 96090214094 74228430120 87765159972 90004630580 4277181196

Table IV. Domain parameters generation and key generation based domain parameters ($F2^m$)

Published by: The Mattingley Publishing Co., Inc.

January - February 2020
ISSN: 0193-4120 Page No. 16907 - 16916

BIT S	Sender's		Receiver's		Shared key
	Secret key	Public key	Secret key	Public key	
163	757512 154461 911949 311096 650501 103099 365131 515204 6	X=620772760 47807232744 42784849734 40205673647 1384876 Y=506399981 48603655484 38596751803 61300334875 3826463	75627087 85871900 89548320 00102293 77259736 81746098 5	X=567502680 464379315723 043967678016 027202873799 9166 Y=900304473 670227028513 137909031033 867164746329 6227	X=962009230 863465564477 680130487471 702119635467 8683 Y=395380773 780606202167 315060372083 471297671209 1949
233	443458 052610 075029 491511 883668 441057 268961 559453 513581 555748 619875 9439	X=709805742 06623124280 22390986881 61541242342 00657518405 34247225457 018793 Y=338204657 58107100795 12597938937 08653118777 69575576739 35242031764 238735	85262187 50404500 77223278 85371381 22624559 69435750 57446032 57695912 53547	X=136528922 684369159949 572939921504 759510008122 125897172838 134465648138 48 Y=135664415 158843382025 055713326033 343021057242 495632591719 516620381178 85	X=690969468 182090132387 112276470905 655174207675 628660323279 449466782742 6 Y=680996624 979009003751 965555243013 409933969066 648210298027 008349916205
283	918826 200479 377074 573925 998425 940382 513248 184745 806377 519432 482673 308222 504150 622463 0	X=155293980 70740236088 27665271898 77748396856 47467329087 95608984280 96245920313 24120701529 Y=697527595 10786813512 31785474977 94065902048 85695409388 72894026495 58234583669 6888379617	73823178 80714955 67213655 60129031 89455826 33726053 39077513 21712033 94625867 26732177 84907	X=318723831 036981680771 927012920504 811045676551 815811632652 691038704543 509283100387 3427 Y=144903043 493209113732 908948509652 593360920174 605357842608 174817380886 723041757442 36142	X=135225456 698651111834 990137611464 445526635566 947288605955 951978123878 987015413803 86448 Y=142103922 712801186343 251022128112 087790118813 614065447084 418395316179 001260228910 42822
409	467886 763777 211769 062957 555245 829600 292427 256437 127315 418656 352835 902546 392970 518972 452862 772594 958027 030861 755170 122397 822	X=471149384 18341045041 12079138936 92932640372 94647782803 35893459067 47032809235 41822712195 13651455764 61902922104 71018080366 1363 Y=268138803 87855715702 52411167892 94105998117 32811055099 79572804855 77433378444 96060972208 12810349030 34559606201 47677546723	11295768 01099988 98148825 62226824 34864366 76178562 69933179 69887986 22205603 06102092 93947121 95604131 71930988 43514573 89681333 7534	X=974752493 692323667190 303082927739 911496927328 567364152070 623621800533 561984617732 108907165148 994898190108 278707119922 298679Y=860 599673548082 128324745486 535392180884 267513446917 308314296357 022717336300 096006246395 294360111444 322810220205 504095654925	X=127503363 590223757331 149325843478 960510462539 070341265256 627841101427 802051028047 491263283072 865259893419 938551785185 3909933 Y=107679814 213993028509 421671387120 100458043585 139865641506 494106406135 573785325678 735969856286 925749506802 359422132825 7601453

BIT S	Sender's		Receiver's		Shared key
	Secret key	Public key	Secret key	Public key	
		5385			
571	316861 732569 892854 669828 095164 527102 834922 510532 488583 551359 218496 379371 930782 594065 377290 527311 595892 004331 570005 211301 460861 571083 828301 213423 105627 127782 795626 757787 1676	96638471405 91949921712 63806794188 62433406429 08033424187 95054998114 68747166734 22846966135 84887490 Y=154278107 98497107399 20789864429 09316230070 15139217092 97033145233 21856554688 79053898206 50322770104 76780027984 11839075662 80503515944 32595193784 68290038082 92160761601 253984675	62332516 56635586 38419791 41334396 06011409 66685440 94426218 38109959 76662185 18564661 15530450 13970867 64858357 36398831 58822229 46126940 11642803 27397374 25239402 11528231 65563099 0843	X=471900482 776179114447 001029428085 735998397036 989293529201 287609929659 138289045384 349770092871 119555288329 273485307298 006726437584 846942889692 722069604627 293580606630 2086836 Y=682526655 249915056259 249453445232 888684101829 836711130870 594189593545 968136842507 092167559054 121609759668 143865104440 794720479425 780535968086 389852905678 120136469923 2813653	X=730429283 622278501519 872420390953 292803916843 792328306975 434058171705 985618225990 268341668583 041561957778 021527666639 738833528136 239152104670 695157685632 041137714685 9301127 Y=233518534 719967696720 146655614632 376032972311 263399919645 448215998958 508548494123 506628077741 660759456319 553085372303 542761013514 819961887202 710928663801 920407324307 7355024

Table V.Generation of Private and Public key based on domain parameters for Binary Field GF(2^m)

In table IV and table V presented the implementation domain parameters generation process and generation of pubic keys and private keys based on the parameters along with time required to execute whole process .The total time required to execute the process domain parameter and key generation based domain parameters are as shown in the following table VI and table VII.

Number of bits	Time Required in (ms)
192	41
224	47
256	62
384	156
521	328

Table VI. Time required for domain parameters generation in F(p)

Published by: The Mattingley Publishing Co., Inc.

January - February 2020
ISSN: 0193-4120 Page No. 16907 - 16916

Number of bits	Time Required in (ms)
163	187
233	281
283	435
409	937
571	1859

Table VII. Time required for domain parameters generation in F(2m)

Table VI and table VII shows time required for domain parameter generation and private key ,public key and shared secret key generation in both implementation including prime field and binary field ,by referring for field operation comparatively required less amount of time(approximate 40%) to execute the processes of key generation and domain parameter generation.

CONCLUSION

ECC (Elliptic Curve Cryptography) based agreements provide the maximum and significant strength as compared to any asymmetric (Public) key cryptosystem of public key generation techniques like DSA, RSA, and Diffie-Hellman key exchange. ECC is offered similar level of security with lesser key sizes, computational power as well. Combined route space is a constraint for devices like smart card & wireless devices. The constant expansion of standards agencies is a significant situation for the practice of a crypto-system. Various standard organizations provide assistance to confirm aspects of security and inter-operability of diverse executions of public key based system. There are numerous standard agencies that progress criterions like NIST, SECG and ANSI.ECC (elliptic curve cryptography) underlying the use of finite field types such as GF(p) or GF(2m), so its operational overhead is very low. This procedure work well under constrained environment and provide comprehensive security solution. Thus implementation of identity (ID) based mutual authentication process with key agreement protocol accomplishment using ECC which can be provides enhanced security. This system has the foremost benefit with smaller amount computational & communication cost. It delivers protected procedure of user's anonymity. Due to use of identity based key agreement protocol, it doesn't require verification table at any end. It also offers mutually agreed process of authentication with phase of key agreement. As a result, this system is competent to offer better security & also possible for practical implementation in wireless systems for the phase of communication.

REFERENCES

[1] K.Y. Lam and E. Okamoto, Eds., Fast Algorithms for Elliptic Curve Cryptosystems over Binary Finite Field "Published in Advances in Cryptology–ASIACRYPT'99, vol. 1716 of Lecture Notes in Computer Science, pp. 75–85, Springer-Verlag, 1999.

[2] B.S. Adiga, Balamuralidhar P, Rajan M. A., RavishankaraShastry, Shivraj V L "An Identity based Encryption using Elliptic Curve Cryptography for Secure M2M Communication" ACM Journal IPICS Oct. 2012.

[3] PritamGajkumar Shah "Investigating Effects of Co-ordinate System on Execution Time of Elliptical Curve Protocol in Wireless Sensor Networks" 2012 International Conference on Future Communication Networks, 978-1-4673-0260-9/12/, 2012 IEEE.

[4] SECG SEC1, Elliptic Curve Cryptography, Standards for Efficient Cryptography Group, ver. 2, 2009, http://www.secg.org/download/aid-780/sec1-v2.pdf.

[5] ShenGuicheng, ZhengXuefeng "Research on the Implementation of Elliptic Curve Cryptosystem Based on Object-Oriented Method" 978-1-4244-2108-4/08, 2008 IEEE.

[6] SihamEzzouak, Mohammed Elamrani and AbdelmalekAzizi "Improving Pollard's Rho Attack on Elliptic Curve Cryptosystems" 978-1-4673-1520-3/12/$31.00 ©2012 IEEE.

[7] Standards for Efficient Cryptography Group. Recommended Elliptic Curve Domain Parameters.SECG SEC 2 version 2.0, 2010.

[8] Trujillo-V´azquez, M. Morales-Sandoval, M.A. Nu˜no-Maganda and M. Ruiz- M´endez "Elliptic

Published by: The Mattingley Publishing Co., Inc.

January - February 2020
ISSN: 0193-4120 Page No. 16907 - 16916

Curve Cryptography onWindows CE devices" 978-1-61284-1325- 5/12.2012 IEEE.

[9] Wasim A, Al-Hamdani, "Elliptic Curve for Data protection" information security curriculum development conference 2011, ACM 978-1-4503-0812-0/10/11.

[10] V. Gayoso Martınez, L. Hern,ezEncinas "Implementing ECC with Java Standard Edition 7" International Journal of Computer Science and Artificial Intelligence Dec. 2013, Vol. 3 Iss. 4, PP. 134-142.

[11] Xia Lin "The Application of Elliptic Curve Cryptography in Electronic Commerce" 2012 IEEE Symposium on Electrical & Electronics Engineering (EEESYM) 978- 1-1673-2365-9/12, 2012 IEEE.

[12] Adnan Abdul-Aziz Gutub "Remodeling of Elliptic Curve Cryptography Scalar Multiplication Architecture using Parallel Jacobian Coordinate System" International Journal of Computer Science and Security (IJCSS), Volume (4) : Issue(4) 409.

[13] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone "HANDBOOK of APPLIED CRYPTOGRAPHY" CRC Press, 2nd edition, 1996.

[14] Dheerendra Mishra, Ashok Kumar Das, SouravMukhopadhyay, "A secure and efficient ECC-based user anonymity-preserving session initiation authentication protocol using smart card" Peer-to-Peer Netw. Appl. (2016) 9:171–192, DOI 10.1007/s12083-014-0321-z09 December 2014 Springer.

[15] S. U. Nimbhorkar, Dr. L. G. Malik "Comparative Analysis of Authenticated Key Agreement Protocols Based on Elliptic Curve Cryptography" ,B. V. Procedia Computer Science 78 (2016) 824 – 830 doi: 10.1016/j.procs.2016.02.065

[16] S. U. Nimbhorkar, Dr. L. G. Malik "Comprehensive Implementation Of Elliptic Curve Arithmetic Using Binary Field GF(2m) "KasmeraJournal Coverage: Science Citation Index Expanded (Impact Factor: 0.071) ,ISSN: 0075-5222 ,published in Vol. 44 (no 6, Year 2016) .

[17] ShanthaA ;Renita J ; Edna Elizabeth N"Analysis and Implementation of ECC algorithm in Lightweight Device" 2019 International Conference on Communication and Signal Processing (ICCSP)DOI: 10.1109/ICCSP.2019.8697990

[18] MashrufeeAlam, IsratJahan, IsratJahan, IsratJerin"A Comparative Study of RSA and ECC and Implementation of ECC on Embedded Systems"International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2763 Issue 03, Volume 3 (March 2016).

[19] Certicom, Standards for Efficient Cryptography, SEC 2: Recommended Elliptic Curve Domain Parameters, Version 1.0, September 2000, Available at http:// www.secg.org/download/aid-386/sec2_final.pdf

[20] D. Hankerson, A. Menezes and S. Vanstone "Guide to Elliptic Curve Cryptography" 2004. Springer ISBN: 0{387{95273{X}.

[21] Fahad Bin Muhaya, Qasem Abu Al-Haija, and Lo'aiTawalbeh" Applying Hessian Curves in Parallel to improve Elliptic Curve Scalar Multiplication Hardware". International Journal of Security and Its Applications Vol. 4, No. 2, April, 2010.

[22] Ion TUTANESCU, Constantin ANTON, Laurentiu IONESCU, Daniel CARAGATA "Elliptic Curves Cryptosystems Approaches" International Conference on Information Society (i-Society 2012) 978-1-908320-05/6, 2012 IEEE.

[23] J. M. Miret_, R. Moreno, J. Pujolàs and M. Valls "Algorithms and cryptographic protocols using elliptic curves" CONTRIBUTIONS to SCIENCE, 3(4):481-491 (2007) Institutd'Estudis Catalans, Barcelona DOI: 10.2436/20.7010.01.24 ISSN: 1575-6343 www.cat-science.cat

[24] Joppe W. Bos, J. Alex Halderman, Nadia Heninger, Jonathan Moore, Michael Naehrig, and Eric Wustrow "Elliptic Curve Cryptography in Practice" CRYPTO, volume 2139 of LNCS, pages 190-200. Springer, 2013

[25] Andre Weimerskirch, douglasstebila, SheuelingchangShantz "Generic GF(2m) arithmetic in software and its Application to ECC" the 8th Australasian conference on Information security and Privacy (ACISP2003).

[26] Anoop M.S. "Elliptic Curve Cryptography An Implementation Guide standards and exercise ",author PHI, fourth version.