International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 5 139 – 144

Cloud Data Security using Elliptical Curve Cryptography

Dr. P. Srivaramangai
Director & Assistant Professor
Srimad Andavan Arts and Science College (Autonomous)
Trichy, Tamilnadu, Inida

J. Rajeshwari
Research Scholar
Srimad Andavan Arts and Science College (Autonomous)
Trichy, Tamilnadu, Inida
rajee.jnr@gmail.com

***Abstract*—**Internet today is seeing a touchy development because of expanded use. In any case, it is helpless against eavesdropping which represents a risk to privacy and security of the client. The security of data traffic winds up plainly vital since the communications over open network happen frequently. It is along these lines basic that the data traffic over the system is encrypted. Since the wireless and wired IP networks are defenseless against eavesdropping, cryptographic plans are produced to secure the information transmitted in a network. To give the quality of service, the cloud computing security is the essential part of the cloud service providers. Nonetheless, cloud computing postures numerous new security challenges which have not been all around researched. This research work concentrating on issues identifying with the cloud data storage strategies and security in virtual condition. We propose a technique for giving data storage and security in cloud utilizing Elliptical Curve Cryptography ECC. Encourage, depicts the security services incorporates generation of key, encryption and decryption in virtual condition.

Keywords-*Multi Level Encryption, Elliptical Curve Cryptography, Particle Swarm Optimization, Bit Sequence*

*****

I. INTRODUCTION

Cloud computing today is seeing a hazardous development because of expanded utilization. In any case, it is defenseless against eavesdropping in which represents a risk to security and protection of the client. The security of information movement ends up plainly critical since the correspondences over open system happen much of the time. It is along these lines fundamental that the information movement over the system is encrypted.

Since the wired and remote IP networks are helpless against eavesdropping, cryptographic plans are created to secure the information transmitted in a system. In this way a stream cipher technique is utilized to encrypt the information transmitted in a system.

Stream cipher is a symmetric key encryption where each piece of information is encrypted with each piece of key. The Crypto key utilized for encryption is changed arbitrarily so that the cipher content delivered is scientifically difficult to break. The changing of arbitrary keys won't permit any example to be rehashed which would provide some insight into the saltine to break the cipher content. The stream cipher can be either equipment arranged [1] [2] [3] or programming focused [4]. A portion of the product situated stream cipher strategies proposed in writing incorporate RC4, Vernam cipher , Fast and secure stream cipher and Key pooled RC4.

RC4 calculation is powerless against expository assaults of the state table. The disadvantage of this calculation is that one in each 256 keys can be a powerless key. These keys are recognized by cryptanalysis that can discover conditions under which at least one created bytes is unequivocally corresponded with a couple of bytes of the key [5]. Likewise the initial three expressions of the secret key can be found and by emphasis each expression of the key utilized as a part of RC4 can be acquired [6].

Vernam cipher [7] is a sort of one-time cushion thought to be an impeccable cipher . Both the sender and the beneficiary have a similar arrangement of keys to encrypt and unencrypt the message. The keys for encryption are produced utilizing an irregular number generator. The keys are an arrangement of non-rehashing grouping of random numbers. Each letter in the plain content has a numeric equal. The encrypted content is the XOR operation of the characters of the plain content with the relating stream of arbitrary numbers. The disadvantage is that the length of the key and the plain content ought to be the same. In this way a substantial number of keys must be put away and appropriated. Additionally if the irregular number arrangement is found, the key utilized for encryption can be followed effortlessly [7].

II. RELATED WORKS

Biham et al., [8] proposed a quick and secure stream cipher for encryption. This strategy depends on another sort of primitive, called Rolling Arrays. It additionally incorporates variable turns and stages. The security cases of the cipher are that no key recuperation assaults can be performed with multifaceted nature littler than that of comprehensive inquiry, and recognizing assaults are additionally unfeasible with a comparable many-sided quality. It is additionally demonstrated that the velocity of the cipher is stunningly quick when contrasted with RC4. The downside in this strategy is that an aggregate of 256 keys must be put away for beginning change. Additionally the key stream produced does not rely on upon the plain content to be encryptd and the plain content is not encoded.

Kim et al., [9] proposed a strategy to execute and assess an effective RC4 stream cipher, called key-pooled RC4, to exchange safely sight and sound documents in the remote versatile system. In this strategy, a 1MB-sized key stream pool, which comprises of 2048 or 8192, or 32768 key stream edges, is made particularly for every customer gadget in the enrollment step. At the point when a customer demands an interactive media record, the server conveys the document in the wake of scrambling it utilizing the succession of key stream outlines which are haphazardly chosen from the relating key stream pool. It is likewise demonstrated that the proposed plan is additional time effective than the typical RC4 and more secure than ordinary RC4. The downside in this strategy is that the quantity of key stream edges to be put away and disseminated is huge.

Wu et al., [10] proposed a technique for encoding pictures utilizing a stream cipher strategy. In this technique a pseudo arbitrary number generator is utilized to create the keys for scrambling the pictures. Likewise Huffman coding strategy is utilized to encode just the plain picture. The disadvantage of this approach is that the keys can be found if the pseudo arbitrary number generator is split.

Sreelaja and Pai [11] proposed an Ant Colony Optimization (ACO) [12] based calculation for key era. The calculation depends on the dissemination of characters in the plain content. The downside is that the vitality estimation of the subterranean insect specialist should be found each time the pheromone statement is updated, by checking the event of characters of the key stream in the plain content. This normally builds the encryption time when the length of the key stream picked is extensive.

III. PARTICLE SWARM OPTIMIZATION

Particle Swarm Optimization (PSO) [13] is a populace based stochastic optimization method roused by social conduct of flying creature rushing or fish tutoring. The PSO framework is instated with a populace of random solutions and scans for optima by updateing eras. In PSO, the potential solutions called particles fly through the issue space by taking after the present ideal particles. Particle swarm has two essential operators to be specific position update and velocity update. Amid every era, every particle is quickened toward the particle's past best position and the worldwide best position. At every emphasis another velocity an incentive for every particle is cipher in view of its present velocity, the separation from its past best position, and the separation from the worldwide best position. The new velocity esteem is then used to ascertain the following position of the particle in the inquiry space. This procedure is then iterated a set number of times until an answer is gotten

IV. PROPOSED MULTI LEVEL ENCRYPTION FOR CLOUD DATA SECURITY

The proposed multi-level encryption authentication scheme contains three main sections.

- Key Establishment using Elliptic Curve
- Generation of Pseudo Random Bit Sequence based Particle Swarm Optimization
- Enhanced Encryption Process

A. Key Establishment using Elliptical Curve Cryptography

In this stage, a secret key is arbitrarily chosen from the key pool and traded amongst sending and accepting hubs. The key foundation stage utilizes an elliptic bend over prime field to create a substantial key pool for hub confirmation reason. An elliptic bend over prime field is an arithmetical expression and is characterized by the accompanying condition:

$$y^2 (mod\ p) = x^3 + Ax + B\ (mod\ p)$$

where, An and B are the coefficients and the factors x and y take the qualities just from the limited field inside the scope of prime field p. Given the estimations of these parameters, a substantial number of focuses on the bend can be created utilizing essential elliptic bend operations, known as point expansion and point multiplying [14].

B. Generation of Pseudo Random Bit Sequence based PSO

The Particle swarm improvement Key Generation calculation (PKGA) is a novel way to deal with produce key stream for content encryption. A Particle swarm model is utilized to pick the key stream for content encryption. A particle swarm model is instated with a gathering of arbitrary particles (arrangements) and after that scans for optima by updateing eras. A particle has N measurements where N takes an estimation of 94. Each measurement in the particle is involved or can be void. The possessed measurement has a character. The gathering of characters in the particle means the particle key stream. The quantity of characters picked in the particle key stream ought to be not exactly or equivalent to the length of the plain content. The position of the particle is found by including the quantity of characters the particle enter stream happening in the plain content. The likelihood of event of characters of the key stream in the plain content is found by partitioning the particle position with the particle key stream length. A base likelihood estimation of 0.75 is picked so that the keys in the key stream happening in the plain content are encoded utilizing the transformed character code table. On the off chance that the likelihood esteem is lesser than the base likelihood esteem, a velocity is given to the particle. Every particle has a velocity key stream related with it. A velocity key stream is a connection of characters of the velocity given to the particle. At first the velocity key stream of the particle is unfilled.

The velocity key stream is meant utilizing N measurements where the estimation of N ought to be equivalent to or lesser

 ISSN: 2321-8169
139 – 144

than length of the plain content short length of the particle key stream if the length of the plain content is lesser than 94. On the off chance that the length of the plain content is more noteworthy than 94, then the estimation of N ought to be lesser than or equivalent to 94 short length of the particle key stream. The characters meaning the velocity key stream involving the measurements in velocity ought to be exceptional.

A velocity is given to the particle to make it move to another position. Each time a velocity is given to the particle a gathering of characters not happening in the particle key stream and velocity key stream are taken. The quantity of characters found the velocity ought to be lesser than or equivalent to N short check (possessed measurements of velocity key stream) where N means the greatest number of characters in the velocity key stream. Each time a velocity is given to the particle the characters involve the measurements in the velocity key stream which are vacant.

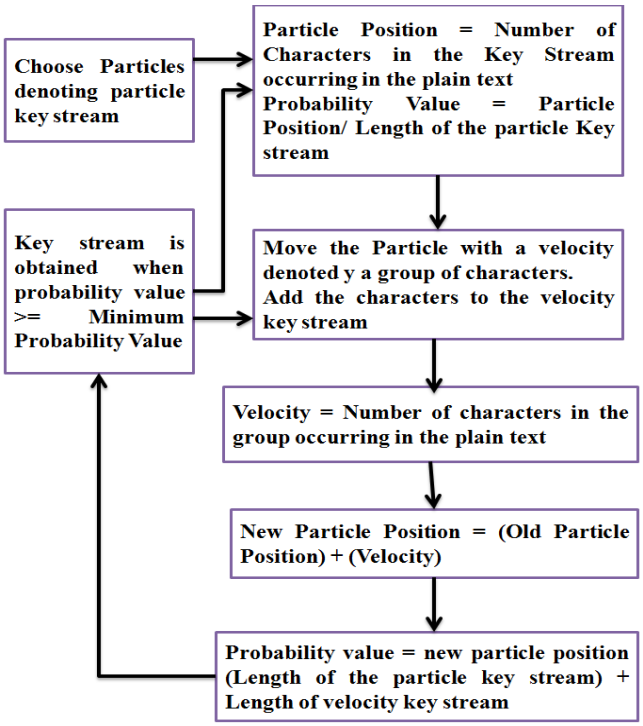

Figure 1: Generation of Key Stream by Particle Swarm Optimization

A tally of the quantity of characters in the gathering happening in the plain content gives a velocity to the particle. These characters indicating the velocity are linked to the characters signifying the velocity key stream. The new position of the particle is found by adding the velocity given to the particle with the old position of the particle. The likelihood esteem is found by separating the new position of the particle with the length of the particle key stream in addition to the length of the velocity key stream. The particle with a most extreme likelihood esteem in an emphasis more noteworthy than the base likelihood esteem is the arrangement and the particle key stream and velocity key stream of the relating particle are linked and picked as the key stream for content encryption.

Pseudo Code for Particle Swarm Key Stream Generation

Step 1: Choose particles with characters denoting the key stream;

$p_i = (X_1, X_2, X_3 \ldots X_{94})$

$VK_i = (VK_1, VK_2 \ldots VK_N)$

Step 2: N = Length of plain text – Particle Key stream length, Length of the Plain text ←94.

Step 3: N = 94- Particle key stream length, Length of plain text > 94

Step 4: Evaluate the position of each particle P_i according to the function

Position (P_i) = count (X_j Є Plaintext), j = 1,2.. Length (P_i)

Step 5: Evaluate the probability value using

probability value (P_i) = Position (P_1)/ Length (P_i)

Step 6: If (Probability Value (P_i) > = minimum probability value) then

Step 7: Return (P_i with probability value (P_i) = maximum probability value);

Step 8: Else

Step 9: Repeat

Step 10: Move the particle to a new position with a velocity

$V_i = (V_1, V_2, V_3..VN_1)$ where

$V_i \neq (P_i, VK_i)$

$N_1 = N – \text{Length}(VK_i)$

New position (P_i) = Oldposition (P_i) + V_i

Step 11: Probability Value (P_i) = New Position (P_i) / (Length (P_i) + Length (VK_i))

$VK_i = VK_i \& V_i$

Step 12: Return (P_i and VK_i with probability value (P_i) = maximum probability value)

Step 13: Until (probability value (P_i) >= minimum probability value);

Step 14: End

C. Enhanced Encryption Process

This enhanced encryption process consists of the following steps:

- Select the secret key from prime field elliptic curve
- BitXOR operation of secret key and secret data bits with logical 1.
- Encryption of Secret key and Secret data using Particle Swarm Key Stream
- Bit shuffling algorithm is used to shuffle the resultant bits (i.e odd as even bits and even bits as odd bits).

ISSN: 2321-8169
139 – 144

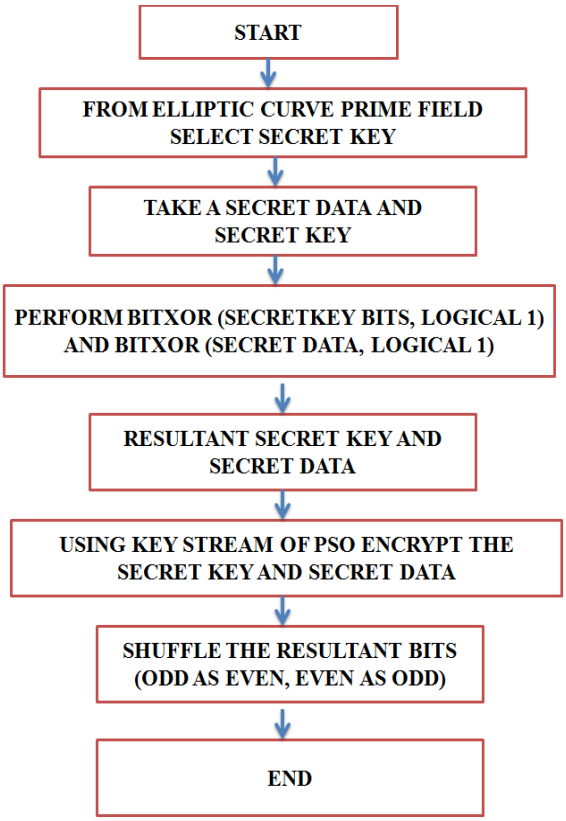

Figure 2: Multi Level Encryption for Cloud Data Security

V. EXPERIMENTAL RESULT AND DISCUSSIONS

Consider the way toward encoding a content utilizing the stream cipher technique in which the key stream for encryption is produced utilizing PKGA. View the content as encrypted is "thisisanopportunity". The base likelihood esteem is thought to be 0.75. Every particle contains characters speaking to the particle key stream. The position of the particle is processed by including the quantity of characters the particle enter stream happening in the plain content. The likelihood esteem is found by separating the particle position by the length of the particle key stream. In the event that the esteem is not as much as the base likelihood esteem a velocity is connected to the particle to move to another position and the position of the new particle and the likelihood esteem is found. The particle with a most extreme likelihood esteem more prominent than or equivalent to the base likelihood esteem in a cycle is the arrangement. The relating particle key stream and velocity key stream are connected which shapes the key stream for content encryption. Table 3 demonstrates the way toward getting the key stream utilizing Particle swarm advancement Key stream Generation calculation. A gathering of particles meaning the key stream are taken. In this the principal particle has a particle key stream "az".

Since 1 character in the particle enter stream happens in the plain content to be encrypted the position of the particle is 1. The likelihood estimation of the particle is observed to be 0.5 which is not as much as the base likelihood esteem. In this way a velocity containing one character "i" is given to the particle to move the particle to another position. Since the character in the gathering meaning the velocity happens in the plain content, the velocity is observed to be 1. This is added to the old position of the particle and the new position of the particle is found to have an estimation of 2. The characters in the gathering meaning the velocity involve the measurements in the velocity key stream. The likelihood esteem is again observed to be 0.66 by partitioning the new position by the total of particle key stream length and the velocity key stream length. Since this is likewise lesser than the base likelihood esteem a velocity is again given to the particle and the procedure is rehashed and the likelihood esteem is observed to be 0.8 which is more prominent than the base likelihood esteem. This methodology is rehashed for different particles in the gathering. Since the main particle in emphasis 3 has the most extreme likelihood esteem 0.8 which is more noteworthy than the base likelihood esteem the particle key stream "az" and the velocity key stream "ips" relating to that particle are linked to shape the key stream "azips" decided for encryption. Each character in the key stream is picked as the key for encryption.

Since the key stream is littler than the length of the plain content to be encoded, the estimations of the keys of the key stream are increased the value of create the keys for the rest of the segment of the plain content. The foreordained esteem can be created by separating the length of the plain content by 2 Since the length of the plain content is 19 the foreordained esteem is computed to be 9. In this illustration, the plain content is isolated into 4 pieces in view of the quantity of characters in the key stream. The quantity of characters of the plain content in each square equivalents the key stream length. The keys in the key stream happening in the plain content are encoded utilizing the secret key. The keys in the key stream that are absent in the plain content are supplanted with their ASCII values. This structures the keys for the plain content in the principal square which measures up to the length of the key stream. The keys for the second square are produced by including the keys of the main piece with the foreordained esteem. So also the keys for the third and fourth square are created by including the keys of the second and third piece individually with the foreordained esteem. Along these lines the keys for the segment of the plain content surpassing the length of the key stream are produced by including the estimations of the keys in the key stream with the foreordained esteem.

The keys utilized for encryption resembles a progression of arbitrary numbers. Utilizing this technique the keys can't be split since the keys relies on upon the characters in the plain content and an arbitrary stream generator is not utilized for key era. In this the quantity of keys in the key stream is 5 and the quantity of sections put away in the character code table to encode the plain content and the keys in the key stream happening in the plain content is 11. In this way a sum of 16

keys must be put away to encrypt a plain content of length 19. Additionally a similar example of keys won't be rehashed.

Table 1: Generation of Key Stream using Particle Swarm System

Particle Key Stream	Position	Probability Value	Velocity	New Position	Velocity Key stream	Probability Value	Velocity	New Position	Velocity Key Stream	Probability Value
az	1	0.5	i-1	2	i	0.66	ps-2	4	ips	0.8
kuyhz	3	0.6	be-0	3	be	0.42	ls-1	4	bels	0.44
lkayt	3	0.6	us-2	5	us	0.7	xz-0	5	usxz	0.55
yagke	2	0.4	lm-0	2	lm	0.29	sb-1	3	lmsb	0.33
Maximum Probability Value		**0.6**				**0.7**				**0.8**

Table 2: Encryption Process

Keys	Blocks Based on Key stream Length	Value for the Keys	Plain Key	Encoded text value from secret key	Cipher Text
a	Block 1	46	T	382	336
z		122	H	383	261
i		190	I	190	0
p		4	S	94	90
s		94	I	190	224
a	Block 2	55	S	94	105
z		131	A	46	173
i		199	N	22	209
p		13	O	10	7
s		103	P	4	99
a	Block 3	64	P	4	68
z		140	O	10	134
i		208	R	3	211
p		22	T	382	360
s		112	U	0	112
a	Block 4	73	N	22	95
z		149	I	190	43
i		217	T	382	423
p		31	Y	1	30

VI. COMPARISON OF ENHANCED ENCRYPTION PROCESS WITH EXISTING METHODS

The stream cipher method using particle swarm system for key generation for encrypting text is compared with the existing stream cipher methods and the stream cipher.

A. Stream Cipher using Particle Swarm Optimization against RC4 Algorithm

A state table is introduced with 1 to 256 bytes to create a pseudo arbitrary stream of keys by swapping the components in the 256 byte state table. A XOR operation between the keys and the plain content delivers the cipher content. The quantity of keys to be put away is less when contrasted with Vernam cipher. These keys can be recognized by cryptanalysis which can discover whether the created bytes are emphatically associated with the bytes of the key.

In the stream cipher strategy utilizing Particle Swarm Optimization Key era calculation, the keys can't be split since the keys created relies on upon the plain content and are encoded utilizing a secret key table utilizing elliptic bend. Since the keys are encoded utilizing character code table, the programmer needs to foresee a hunt of 2t-1 tables to recognize the table utilized for encoding the plain content and the keys in the key stream happening in the plain content where t is the quantity of inward hubs

B. Stream Cipher using Particle Swarm Optimization

In Vernam cipher the keys are haphazardly created utilizing irregular stream generator. The disadvantage is that the quantity of keys to be put away and appropriated ought to be equivalent to the length of the plain content. Additionally the keys used to encrypt the plain content can be found if the arbitrary number generator is split.

In the stream cipher technique utilizing particle swarm streamlining, Particle Swarm System is utilized to produce the key stream for encryption. Despite the fact that the keys utilized for encryption resembles a progression of arbitrary numbers, the keys can't be broken on the grounds that an irregular number generator is not used to create the keys. Likewise the key stream era relies on upon the character appropriation in the plain content defeating the downside of vernam cipher.

Notwithstanding this the stream cipher technique decreases the quantity of keys to be put away and disseminated contrasted with that of vernam cipher when the length of the plain content is substantial. Consider the case talked about in the trial result. The length of the plain content to be encoded is 19. On the off chance that vernam cipher is utilized then an aggregate of 19 keys must be put away and circulated though the stream cipher strategy in view of Particle Swarm System needs just 16 keys to be put away and appropriated.

VII. CONCLUSION

Encryption is a vital issue in today's correspondence since it is completed over the air interface, and is more defenseless against misrepresentation and listening in. Particle Swarm Optimization based approach named upgraded encryption handle for creating key stream to encoding the plain content. Additionally the keys in the key stream are utilized to produce

the keys for the part of the plain content surpassing the length of the key stream. This strategy for encryption utilizing a stream cipher lessens the quantity of keys to be put away and dispersed contrasted with that of vernam cipher . It serves to conquer the disadvantages of the current stream cipher techniques.

REFERENCES

[1] Deepthi.P.P, Deepa Sara John, P.S.Sathidevi, "Design and analysis of a highly secure stream cipher based on linear feedback shift register", Computers and Electrical Engineering, Volume 35, Issue 2, pp 235-243, March 2009.

[2] Hell.M, Johansson.T, Maximov.A. Meier.W." A Stream Cipher Proposal: Grain". IEEE International Symposium on Information Theory, 9-14 July 2006, pp 1614 – 1618.

[3] T. Good and M. Benaissa. "Hardware Results for selected Stream Cipher Candidates". State of the Art of Stream Ciphers 2007 (SASC 2007), pp 191-204.

[4] Common wealth Office of technology, Monthly cyber security tips, Volume 3 Issue 5, May 2008.

[5] A.Roos, "A Class of weak Keys in the RC4 Stream cipher", Vironix Software Laboratories, Westville, South Africa, Sep 1995.

[6] Mantin and A. Shamir, "Weaknesses in the key scheduling algorithm of RC4", Lecture Notes in Computer Science, Vol. 2259, Revised Papers from the *8th Annual International Workshop on Selected Areasin Cryptography*, *pp:* 1 - 24, 2001.

[7] Charles Pfleeger, Shari Lawrence Pfleeger, *Security in computing*, Third Edition 2003, pp 48, Prentice Hall ofIndia Pvt Ltd, New Delhi.

[8] Biham, E. and Seberry, J. "Py (Roo): A Fast and Secure Stream Cipher". EUROCRYPT'05 Rump Session, at the Symmetric Key Encryption Workshop (SKEW 2005), 26-27 May 2005.

[9] HongGeun Kim, JungKyu Han and Seongje Cho. "An efficient implementation of RC4 cipher for encrypting multimedia files on mobile devices". SAC '07 Proceedings of the ACM symposium on Applied computing, 2007, pp 1171--1175, NewYork, USA.

[10] Chung-Ping Wu, C.C. Jay Kuo, "Design of Integrated Multimedia Compression and Encryption Networks", *IEEE Transactions on Multimedia*, Volume 7, Issue 5, Oct. 2005 Page(s): 828 – 839.

[11] B. Schneier, *Applied Cryptography*, *Second Edition : protocols, algorithms and source code in C*, pp 15-16.John Wiley and Sons, 1996.

[12] Sreelaja.N.K and G.A.Vijayalakshmi Pai," Swarm Intelligence based key generation for Text encryption in Cellular Networks". *IEEE Proceedingsof the Third International Conference on SystemSoftware and Middleware* and Workshops, 2008. COMSWARE 2008. 6-10 Jan. 2008. pp: 622 – 629.

[13] Matthew Settles, "An Introduction to Particle Swarm Optimization", Department of Computer Science, University of Idaho, November 7, 2005.

[14] M. Amara and A. Siad, "Elliptic curve cryptography and its applications," in *Proc. 7th Int. WOSSPA*, May 2011, pp. 247–250.

.