Abstract:-

The present study has aimed to explain the changing area under Jowar, Wheat, and Rice crops of Nanded district during 1984-85 to 2009-10. Agricultural is one of the most important occupations of the study area. Nearly 78.13% of working population is directly engaged in agricultural activities. The Economy of the study region mainly depends on agricultural. The modern agricultural implements is improved or hybrids seeds use of different pesticides, insecticides. Weedisides, fungicides and irrigation facilities have increase agricultural production of the study region. Agriculture is more prosperous in the areas of various river basin i.e. Godavari, Manjara, Manyad, Penganga, Asana, Sita, and lendi etc.

Nanded district "kharip" and "Rabbi" both crops are taken in Kharip season hybrid Jowar, Bajari, and Cotton as well as Ground nut crops are mainly taken. During the year 1998-99, studding the cultivated land it was come forward that the percent of area under cultivation of Jowar was 30.15%, Wheat was 2.01%, Rice was 4.75% and Bajara was 0.08% out of the total cultivated land where the area under cereals is 37.09%.

CHANGING PATTERN OF ARICULTURAL LAND UNDER SELECTED CROPS IN NANDED DISTRICT

P. A. Khadke , Varsha Manathkar and P. B Waghmare
Assistant Professor, School Of Earth Sciences,
Swami Ramanand Teerth Marathwada University,
Nanded, Maharashtra.
Research Scholar, School Of Earth Sciences,
Swami Ramanand Teerth Marathwada University,
Nanded, Maharashtra.

Keywords:

Agricultural, occupations, hybrids seeds, pesticides, insecticides, irrigation, production.

P. A. Khadke
Assistant Professor, School Of Earth Sciences,
Swami Ramanand Teerth Marathwada
University, Nanded, Maharashtra.

INTRODUCTION

In this research paper, we will present you that In previous Decade side channel attacks show us that cryptographic Devices are vulnerable or we can say these devices can leak important information. In previous days cryptanalysis assumed that advance user can only has access to data pair which is to be input or output, has no knowledge of the internal state of Device. But today adversary can access the data by using specialized hardware which monitor the device continuously and gain information by timing, electromagnetic emission and power consume of the device. The advance users can gain information without breaking the mathematically operation. They can gain critical information about the internal state of device or operation being performed.

Designers trying to design secure and complex cryptosystems, but new method of tampering and attacks are continuously introduced by the adversaries. They have to only success one out of various methods of tampering data and Designers has to design secure algorithms. Sometimes, the countermeasures of another method arevaluable for new attacks. So we can say the game of Designing complex and secure algorithms and attacks on the new Design is never ending task.

In this paper we will present you a brief summary of recent attacks on Elliptic Curve Cryptography and countermeasures of these attacks. We will introduce only attacks which have been either performed practically or there is a proof of concept of these attacks. We will not introduce any new attack on Elliptic Curve Cryptography. There is no perfect countermeasure against these attacks.

2 BACKGROUNDS

We will present you a summary of new attacks on Elliptic Curve Cryptography.We will also provide you few implementations of new Attacks on ECC. If you want a comprehensive description about ECC then you can find it in [10],[11]. If someone wants to take more information of power analysis attacks according to the class on implemented attacks detected by Cryptographers, we refer you to [8].

We describe here some of the annotations which will be used in this paper.
In this paper some of the notations used are describe according to [9] as follow:

P is a point P with Coordinates x and y
O a point from infinity
The order of point (P) : the smallest integer r such that rP=`O
Affine coordinates: a point is represented with x-axis and y-axis which is represented as a tuple of two integer number (x,y)
Projective coordinates: point (p) is represented as 3D object (X, Y, -Z), but here we use x=X/-Z, y=Y/-Z
Jacobianprojective coordinates: a point (p) is represented as (X, Y, Z), where $x= X/Z^2$, $y= Y/Z^3$

2.1 Elliptic Curve Cryptosystem

Weierstruss equation is use to define an E Elliptic Curve cryptography over finite fields

$$E: y^2 + a1xy + a3y = x^3 + a2x2 + a4x + a6$$

Where a1, a2, a3, a4, a6 are coefficient of finite fields.

2.1 Scalar Multiplication

X(a point with coordinate x-axis, y-axis) , is the point of Infinity makesabelian group with Elliptic Curve (E) where E has the sets of P. so the point X∈E(K) and K (scalar) is a Set of Finite Field), kX is called multiplication of scalar or point of multiplication. ECC security is based on the ECDLP , get k for P and Q such that P=kQ, Where P and Q are two points.

3 Passive Attacks

Elliptic Curve Cryptography is Based on the Elliptic Curve Scalar Multiplication (ECSM). So the main thing is Hardness which provides security of ECC so we can say Security depends on the complexity of the ECSM. When ECSM executes in system or any cryptography enabled device, scalar k can be revealed using various ways or ECSM operation leak the value of k it can be revealed using various methods. The Attacker only wants to get the full bit stream of k by performing physical attack. Physical attack is of two types a. Fault Analysis (FA), b. Side Channel Analysis (SCA).

SCA most attacks use leakage on power consumption. Mainly Electromagnetic (EM) radiation is emphasize to get the leakage when power consumption by device.

3.1 Simple Power Analysis

Simple Power Analysis (SPA) uses the key dependent patterns which are shown in power traces [5]. According to Coron [3], If an adversary can differentiate between the doubling point and addition point from the power trace, which are used in point multiplication using double-and-add algorithm.

3.2 Template Attacks

Template attack [7] isavailable, when you have a device which can be controlled fully and this attack mainly performed in two phases. First one is profiling phase and second is attacking phase. In profiling phase, attacker uses the device and constructs the template. And in attacking phase, attacker does use these templates to get the internal information of the device. The feasibility of this Attack is shown by Medwed and Oswald [37].

3.3 Differential Power Analysis

Differential Power Analysis (DPA) attack gets the sequentially, device with Q input point Xi, i ∊{1,2,…, Q }. The measurement on the device with this input over time is recorded by performing side channel attacks. The attacker chooses any value which lies or depends upon both input point Xi and scalar k. Now the hacker uses Hypothetical Leakage Model to convert this value to a Hypothetical Leakage value. The attacker guesses the value and the correlation between the hypothetical guess and the measurement. With using same method he can get the whole scalar.

3.4 Comparative Side-Channel Attacks

This attack enjoys both attacks Simple SCA and Differential SCA. So we can say it comes under the category both attack of Simple SCA and Differential SCA. In procedure of this attack we first take copy of one stream of bits and then again make a copy of another bit of streams. Now we compare these two traces and it is find out to reuse these values. Doubling attack is the first attack that belongs to this attack [19]. Doubling attack is based on assumption because attacker doesn't know what operation being performed he/she just waits and watches to reoccur the same operation twice.

3.5 Refined Power Analysis

The Special points (x,0) and (0,y) are exploited in Refined Power Analysis attack. Now if we use these two points and feed these points into the device then this point A lead to another point which is a special point B (0,y) at step with assumption that the processed bit will generate the scalar bit stream.

4 COUNTERMEASURES

Many countermeasures has been proposed for protection, however, these countermeasures eliminate the specific issue in existing implementation for a specific attack. Most of the time it has been reported that the countermeasure for one attack may have the benefit for other attack. We will present to you some of the countermeasures for different methods which we described earlier.

4.1 Simple Power Analysis CountermeasureIndistinguishable Point Operation Formula (IPOF)

Difference between point doubling and point addition is eliminated using IPOF but not every time. Basically using add-and-double method it is easily leaked the Hamming weight of the secret scalar [2].

4.2 DPA CountermeasuresScalar Randomization

Private scalar is blinds by adding multipleElliptic Curve [3].

5.CONCLUSIONS

In this paper we give you a summary of the recent attacks on ECC which are performed by adversary. We only present you a brief summary of the attacks. We don't have intension of giving you comprehensive information about the attacks. But we will describe you a details of the attacks which are being performed on ECC. We strongly believe keeping in mindthat all the previous attacks, algorithm designers can help in design and implement of a best security on ECC. We can use it in early stages of the development.

ACKNOWLEDGEMENT

This paper work was under the guideline of Amity Institute of Information Technology, Uttar Pradesh as a part of MCA degree complication. This work is done under the support and guideline of Mr. Himanshu Gupta,Senior Faculty Member, Amity University, sec 125, Noida . Uttar Pradesh.

REFERENCES

1.An Updated Survey on Secure ECC Implementations: Attacks, Countermeasures and Cost Junfeng Fan and Ingrid VerbauwhedeKatholiekeUniversiteit Leuven, ESAT/SCD-COSIC and IBBT KasteelparkArenberg 10, B-3001 Leuven-Heverlee, Belgium
2. Brier, E., Joye, M.: Weierstraß Elliptic Curves and Side-Channel Attacks. In: Naccache,D., Paillier, P. (eds.) PKC 2002. LNCS, vol. 2274, pp. 335–345. Springer,Heidelberg (2002)
3. Coron, J.: Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems.In: Ko¸c, C¸ .K.,Paar, C. (eds.) CHES 1999. LNCS, vol. 1717, pp. 292–302.Springer, Heidelberg (1999)
4. Fouque, P.-A., Valette, F.: The Doubling Attack – Why Upwards Is Better than Downwards. In: Walter, C.D., Ko¸c, C¸ .K.,Paar, C. (eds.) CHES 2003. LNCS, vol. 2779, pp. 269–280. Springer, Heidelberg (2003)
5. Kocher, P.C., Jaffe, J., Jun, B.: Differential Power Analysis. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 388–397. Springer, Heidelberg (1999)
6. Medwed, M., Oswald, E.: Template Attacks on ECDSA. In: Chung, K.-I., Sohn, K., Yung, M. (eds.) WISA 2008. LNCS, vol. 5379, pp. 14–27. Springer, Heidelberg (2009)
7. Chari, S., Rao, J.R., Rohatgi, P.: Template attacks. In: Kaliski Jr., B.S., Ko¸c, C¸ .K.,Paar, C. (eds.) CHES 2002. LNCS, vol. 2523, pp. 13–28. Springer, Heidelberg (2003)
8. Avanzi, R.M., Cohen, H., Doche, C., Frey, G., Lange, T., Nguyen, K., Vercauteren, F.: Handbook of Elliptic and Hyperelliptic Curve Cryptography. CRC Press, Boca Raton (2005)
9. Baek, Y.-J., Vasyltsov, I.: How to Prevent DPA and Fault Attack in a Unified Way for ECC Scalar Multiplication – Ring Extension Method. In: Dawson, E., Wong, D.S. (eds.) ISPEC 2007. LNCS, vol. 4464, pp. 225–237. Springer, Heidelberg (2007)
10. Akishita, T., Takagi, T.: Zero-Value Point Attacks Elliptic Curve Cryptosystem. In: Boyd, C., Mao, W. (eds.) ISC 2003. LNCS, vol. 2851, pp. 218–233. Springer, Heidelberg (2003)
11. Avanzi, R.: Side Channel Attacks on Implementations of Curve-Based Cryptographic Primitives. Cryptology ePrint Archive, Report 2005 /017,http://eprint.iacr.org/