IJRECE VOL. 4 ISSUE 3 JULY.-SEPT. 2016 ISSN: 2393-9028 (PRINT) | ISSN: 2348-2281 (ONLINE)
DOI: 10.13140/RG.2.1.4354.4566

The Study of Various Applications and several datasets in Elliptic curve cryptography

Saumya Rajvanshi[1],Gurleen Kaur[2], Gurjot Singh Sodhi[3]
[1]*M.Tech(Student), Udham Singh College of Engineering and Technology, Tangori, Mohali*
[2]*Assistant Professor, Shaheed Udham Singh College of Engineering and Technology, Tangori, Mohali*

Abstract- Elliptic curve cryptography is established on the data encryption/decryption, they are most widely used in video conferencing, privacy of information other social broadcastings and they are the effective one that deal with the confidentiality of data and are peak widely used to examine, invention the methods for security of data. ECC is a kind of public key cryptosystem similar to RSA. Then it contrasts from RSA in its earlier evolving capacity and by providing attractive and alternative technique to investigators of cryptographic procedure. The security level which is given by RSA can be provided even by smaller keys of ECC. The principal attraction of elliptic curve cryptography compared to RSA is that it offers equal security for a smaller key-size. Symmetric ciphers is based on the size of the key and the same keys are used to encrypt and decrypt data .Asymmetric ciphers consist of two different keys where one is the public key and secretive key. The safety is based upon the segment and the exponent used.

Keywords- Ecliptic Curve Cryptography, data decryption, Symmetric ,information encryption and Asymmetric ciphers.

I. INTRODUCTION

A lot of work has been done on ECC meanwhile formerly. An elliptic curve captivates a lot of cryptographic effort owing to the statistic that regardless of the use of slighter keys they deliver similar level of safety than RSA or key altercation procedure like Diffie-Hellman. ECC kinds use of elliptic curve distinct over a limited field. A limited field confines the mutable and constants to its fundamentals. Elliptic Curves remain not abbreviations, and are not to be disordered through them. The individual feature that elliptic curves segment with an ellipse is the environment of equation that produces the elliptic curve. [1] The advantage of ECC over its competitors increases, as the safety requirements increase in excess of time. Here we present Diffie_hellman key exchange algorithm providing forward privacy for web browsers request. DHKE is a exact method of exchanging cryptographic keys, allows two parties that have no previous information of each additional to jointly launch a shared secret key over an insecure communications channel. This strategic container then be used to encrypt following communications using a symmetric key cipher.[2]

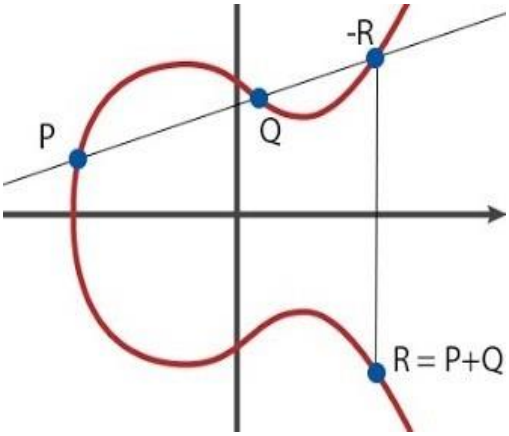

Fig. 1 of Elliptic Curves in Cryptography

Advantages of ECC

1. superior flexibility in selecting cryptographic structure
2. no known sub exponential time algorithm for ECDLP ⇒ smaller key dimensions (with the same safety). Current reference (according to A.K. Lenstra, E.R. Verheul): the smallest key size for ECC must be 132 bits vs. 952 bits aimed at RSA.
3. As a result: greater speed, less storage ⇒ ECC can be used in insolent cards, cellular telephones, pagers etc.
4. Scope of the Key: Key of the scope required for encryption and digital signature is mainly far lower than other system.
5. Shorter Time for encryption
6. Currently know the techniques for the solution of DL difficulties can be applied. The use of Brute force attack on eclipse curve cryptography takes a lot longer time to be effective.
7. Any cryptographic rules and scheme depend upon discrete logarithms can be easily converted to elliptic curve form.
8. If order is fixed point F is an n-bit prime, then computing k from k*F and F takes approximately 2 ^ (n/2) operations [3].

Disadvantages

1. Hyper elliptic cryptosystems offer even smaller key sizes.
2. ECC is mathematically more subtle than RSA or SDL ⇒ difficult to explain/justify to the client.

DOI: 10.13140/RG.2.1.4354.4566

3. ECC uses elliptic curve, generators and finite fields and point of curve, which can lead to more difficult calculations that could strain an added processor.
4. Circumvented with lookup stands for elliptic curves, but this can eat up valuable resources on handheld and movable devices. Filed has not been verified mainly, calculate the other fields. [4]
5. Probability of n future discovery of sub exponential attack. An effective discovery of an attack on system can weak the protection of the system.
6. ECC system is slower than RSA in public key procedures. So in submissions requiring enormous encryption the system is not needed.

II. SEVERAL LARGE CRYPTOGRAPHIC DATASETS

- The first (and largest) dataset is gotten from the Bit coin chunk restraint. Bit coin is an electronic crypto-currency, and elliptic curve cryptography is dominant to its process: Bit coin speeches are straight derived from elliptic-curve public keys, and communications are genuine using digital monograms. The public keys and monograms are published as part of the publicly available and auditable chunk cable to avoid double-spending.
- The second largest dataset we collected is drawn from an Internet-wide examination of HTTPS systems. Elliptic-curve cipher groups that offer forward confidentiality by launching a sitting key with elliptic-curve Diffie-Hellman key exchange were introduced in 2006 and are growing in admiration for TLS. This dataset comprises the Diffie-Hellman system key exchange information, as well as public keys and signatures from systems via ECDSA.
- We also achieved an Internet-wide examination of SSH systems.Elliptic-curve cryptograph collections for SSH were presented in 2009, besides are also rising more shared as software provision rises. This dataset comprises elliptic curve Diffie-Hellman scheme key exchange information, elliptic-curve public cloud keys, and ECDSA signatures [4].
- Finally, we collected credential info, including open keys from the publicly available lightweight directory access protocol (LDAP) record for the Austrian Resident Card. The Austrian e-ID contains public keys for information encryption and ordinal signatures, and as of 2009, ECDSA signatures are offered.

III. RELATED WORKS

Aditya Babel et.al,2010 [5] The basic structures of elliptic curve cryptography deprived of successful into the complex mathematical information is expored. They advance some mathematical theory in describing elliptic curve collections and their interior operations. Through this paper, they compare ECC to other asymmetric encryption structures such as RSA and ELgamal and, in doing so, hope to influence the reader that, despite its somewhat disgusting and complicated look, ECC is indeed a consistent cryptographic scheme that will be significant in the near future.

Haodong Wang et.al,2006 [6] this paper describes a public key implementation of access control in a sensor network. They detail the implementation of Elliptic Curve Cryptography over primary field, a public-key cryptography scheme, on TelosB, which is the modern sensor network platform. They appraise the performance of implementation and compare with other operations we have ported to TelosB.

IkshwansuNautiyal et.al, 2012 [7] in this article described as, Cryptography is the method of hiding a message in some indecipherable format so that the message lies hidden in plain sight of an accidental person. The methods of cryptography are centuries old. With technical development, techniques have evolved knowingly. Public key cryptography offers a wide variety of safety over the various methods of transferring data, especially over Internet. The security of a public key encryption is stronger only if the validity of the public key is ensured. Data encryption values like RSA and Diffie- Hellman are becoming incompetent due to requirement of large quantity of bits for cryptographic process. As of newest, ECC has developed the latest tendency in the cryptographic situation. This paper presents the operation of ECC for encryption or decryption and confirmation process, using JAVA as the implementation tool.

Joppe W. Bos et al., 2013[8] They perform a evaluation of elliptic curve cryptography ,as it was used in repetition, in order to reveal unique errors and susceptibilities that arise in operations of ECC. They study four popular procedures that make use of this type of public-key cryptography: Bit coin, endangered shell transport layer security and the Austrian e-ID card. They were pleased to observe that about 1 in 10 systems sustenance ECC across the TLS and SSH protocols. However, they find that notwithstanding the high stakes of money, access and properties protected by ECC, executions suffer from vulnerabilities similar to those that disease previous cryptographic system.

EmiliaK¨asper et al., 20011 [9] presented a 64-bit improved implementation of the NIST & SECG consistent elliptic curve P-224. They application was fully combined into Open SSL 1.0.1: full TLS handclasps using a 1024-bit RSA credential and ephemeral Elliptic Curve Diffie-Hellman key exchange over P-224 now run at double the speed of typical Open SSL, while microscopic elliptic curve measures were up to 4 times faster. In addition, implementation was protected to timing attacks—most notably, they expression how to do small table look-ups in a cache-timing unaffected way, allowing us to use pre-computation.

Moncef Amara et al., 2011[10] Elliptic Curve Cryptography, and in what way it's a better promise for a quicker and more secure method of encryption in evaluation to the current values in the Public-Key Cryptographic procedures of RSA was

DOI: 10.13140/RG.2.1.4354.4566

deliberated in this paper. The Elliptic Curve Cryptography protections all relevant asymmetric cryptographic primitives like digital signatures and key agreement processes. The function used for this determination was the scalar multiplication k.

IV. APPLICATION OF ELIPTIC CURVE

In this unit, we survey utilizations of elliptic curve cryptography in the real biosphere and deliver statistics on usage.

A. Bitcoin

The crypto-currency Bit coin is a dispersed peer-to-peer ordinal currency which allows "online payments to be sent straight from one

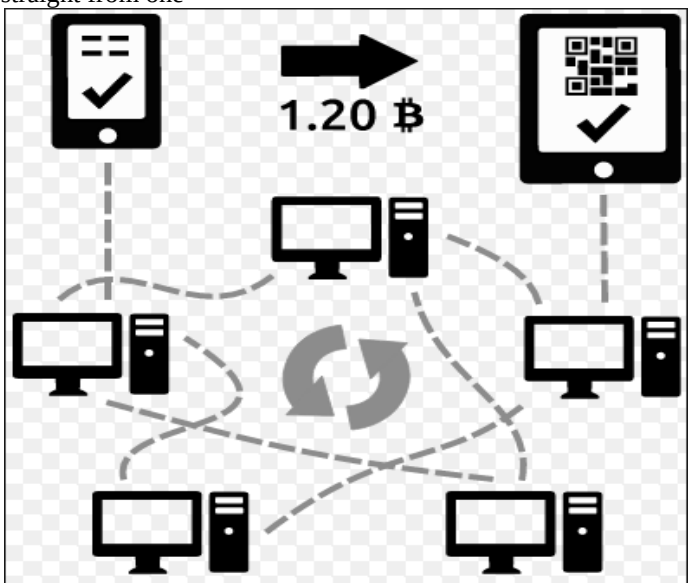

Fig. 2 Bit coin working

gathering to another without profitable through a financial institution" [4]. The (public) Bit coin block chain is a periodical of all the dealings ever performed. Each block in this journal contains the SHA-256 [5] hash of the preceding block, hereby binding the blocks composed starting from the so-called genesis block. In Bit coin, an ECDSA secretive key characteristically works for as a user's account. Transferring ownership of bit coins from user A to user B is understood by ascribing a digital autograph (using user A's private key) of the hash of the previous transaction and info about the unrestricted key of user B at the end of a novel operation. The signature can be verified with the assistance of user A's open key from the preceding transaction. Additional issues, such as avoiding twice expenditure, are deliberated in the original article.

B. Secure Shell (SSH)

Elliptic curve cryptography can be used in three positions in the SSH procedure. In SSH-2, assembly keys are transferred using a Diffie-Hellman key exchange. RFC 5656 [48] specifies the transient Elliptic Curve Diffie-Hellman key conversation technique used in SSH, behind SEC1 [7]. Each server has a host significant that permits the server to validate it to the consumer. The attendant sends its cloud key to the client throughout the key conversation, and the user confirms that the key impression competitions their saved value. The server then authenticates itself by ratification a copy of the key conversation. This cloud key might be an ECDSA public key [48]. Finally, clients can use ECDSA public keys for client authentication.

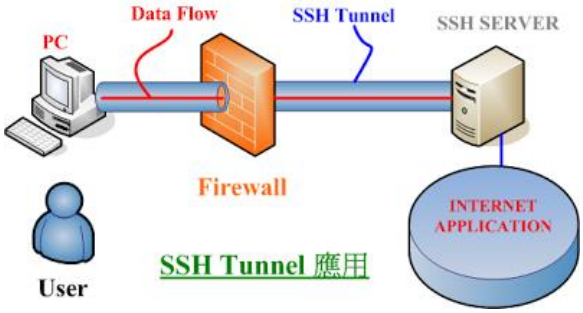

Fig no 2 Secure Shell (SSH)

C. Transport Layer Security

In TLS, elliptic curves can rise in several sites in the protocol. RFC 4492 [9] stipulates elliptic curve cipher collections for TLS. All of the cipher collections quantified in this RFC usage the elliptic curve Diffie-Hellman (ECDH) key conversation. The ECDH keys may either be long-term (in which situation they are discarded for dissimilar key interactions) or ephemeral (in which case they are regenerated for each key conversation). TLS documentations also cover a public key that the system uses to authenticate itself; with ECDH key exchanges, this public key may be either ECDSA or RSA.

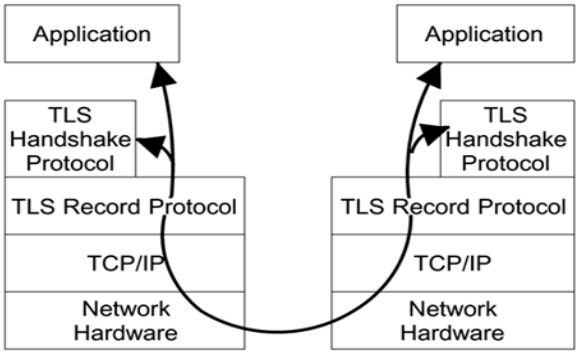

Fig. 3 Transport Layer Security

V. ELLIPTIC CURVE CRYPTOGRAPHY TECHNIQUES

1) ECDSA - Elliptic Curve Digital Signature Algorithm: Signature algorithm is used for authenticating a device or a message sent by the device. For example consider two

DOI: 10.13140/RG.2.1.4354.4566

devices[8] A and B. To authenticate a message sent by A, the device A symbols the message using its confidential key. The tool A sends the message and the signature to the device B. This signature can be established just by using the communal key of device A. Since the device B knows A's public key, it can confirm whether the message is certainly send by A or not. ECDSA is a variant of the Digital Signature Algorithm (DSA) that functions on elliptic curve collection. For distribution a signed message from A to B, both have to agree up on Elliptic Curve domain constraint. The domain constraint are definite in section 9. Sender 'A' have a key pair consisting of a private key dA (aarbitrarily selected digit less than n, where n is the order of the curve, an elliptic curve domain parameter) & a communal key QA = dA * G (G is the producer point, an elliptic curve domain parameter). An overview of ECDSA process is defined follow.

- Signature creation For signing a message m by sender A, using A's private key dA 1.
- Calculate e = HASH (m), where HASH is a cryptographic hash meaning, such as SHA-1 2.
- Select a random integer k from [1,n − 1]
- Calculate r = x1 (mod n), where (x1, y1) = k * G.
- If r = 0, go to step 2 4. Calculate s = k − 1(e + dAr)(mod n). If s = 0, go to step 2
- The signature is the pair (r, s)

Signature Verification for B to authenticate A's signature, B should have A's communal key QA

1. Confirm that r & s are integers in [1,n − 1]. If not, the signature is invalid
2. Calculate e = HASH (m), wherever HASH is the similar function used in the signature generation
3. Calculate w = s −1 (mod n)
4. Calculate u1 = ew (mod n) and u2 = rw (mod n)
5. Calculate (x1, y1) = u1G + u2QA
6. The signature is valid if x1 = r(mod n), invalid otherwise

2) ECDH – Elliptic Curve Diffie Hellman: ECDH is a key agreement protocol that allows two parties to found a shared covert key that can be used for confidential key algorithms. Both parties exchange some public information to all other. Using this public information & their possess private data these parties calculates the shared secret. Any third gathering, who doesn't have contact to the private information of each device, will not be capable to determine the shared covert from the available public information.[9]

An overview of ECDH process is defined below. For generating a shared secret among A & B using ECDH, together have to agree up on Elliptic Curve area parameters.

Together end have a key pair consisting of a confidential key d (a randomly chosen integer take away than n, where n is the arrange of the curvature, an elliptic curvature domain stricture) & a public key Q = d * G (G is the producer point, an elliptic curve domain parameter).

Let (dA, QA) be the confidential key - communal key pair of A & (dB, QB) be the private key - public key pair of B[10].

1. The end A compute K = (xK, yK) = dA * QB
2. The end B compute L = (xL, yL) = dB * QA
3. Since dAQB = dAdBG = dBdAG = dBQA. Consequently K = L and hence xK = xL
4. Therefore the shared covert is xK Since it is practically impossible to find the private key dA or dB as of the communal key K or L, it's not probable to obtain the shared secret for a third party

3) Why ecc is better?

Elliptic Curve Cryptography (ECC) is one of the most powerful but least understood types of cryptography in wide use today. At Cloud Flare, we make extensive use of ECC to secure everything from our customers' HTTPS connections to how we pass data between our data centers. Fundamentally, we believe it's important to be able to understand the technology behind any security system in order to trust it. To that end, we looked around to find a good, relatively easy-to-understand primer on ECC in order to share with our users. Finding none, we decided to write one ourselves.

- Smaller keys, cipher texts and signatures.
- Very fast key generation.
- Fast signatures.
- Moderately fast encryption and decryption.
- Signatures can be computed in two stages, allowing latency much lower than inverse throughput.

4) Comparison between previous and present techniques

When it comes to ECC, the basic operation is point addition, which is known to be very expensive. That makes it very [11] unlikely to discover a sub-exponential attack on ECC in the near future (even though some particular curves of ECC are prone to them and can be avoided easily, as it is quite easy to distinguish them).

Table 1. Comparable Key Size (in bits)

Symmetric Algorithms	ECC	RSA
80	163	1024
112	233	2240
128	283	3270
192	409	7680
256	571	15360

Table2.Comparison key generation performance

Key Length (bits)		Time (s)	
ECC	RSA	RSA	ECC
163	1024	0.16	0.08
233	2240	7.47	0.18
283	3270	9.80	0.27

DOI: 10.13140/RG.2.1.4354.4566

409	7680	133.90	0.64
571	15360	679.06	1.44

Meanwhile, RSA already has a known sub-exponential attack. So, the bits requirement for RSA generated key pair is supposed to rise much faster than that for ECC generated one. Also, for a similar level of security, the numbers involved in ECC are smaller as compared to RSA, as can be derived from the data displayed in tables 1, 2, 3, and 4. Hence, the number of transistors required for security also gets reduced in case of ECC. And since PKC is used to transfer short messages, ECC comes in handy as it is faster than RSA for short messages. The bandwidth requirement becomes quite similar in case of longer messages.

VI. CONCLUSION

Elliptic curve cryptography (ECC) and have industrialized an alphabetic table for ECC data encryption and decryption in a appropriate method. The strong point of encryption is contingent on its key & if we use the alphabetical table formerly around self-control remains no impact on strong point and runtime performance. The opportunity to conveniently use elliptic curve cryptosystems within profitable requests is now only flattering a reality. The arrangement shows that when compared to the security by the exponential-operation procedures, the ECC structure employs far lesser cost for the same safety by the elliptic curve multiplicative operations. The stimulating and rather complex nature of elliptic curve collections makes it harder to crack the ECC discrete logarithm problematic. With less bits required to give the same security, ECC has fared favorably compared to either RSA.

VII. REFERENCES

[1]. Roy, Sudipta, et al. "International Journal of Advanced Research in Computer Science and Software Engineering." International Journal 3.6 (2013).

[2]. Ahirwal, Ram Ratan, and ManojAhke. "Elliptic curve diffie-hellman key exchange algorithm for securing hypertext information on wide area network."International Journal of Computer Science and Information Technologies 4.2 (2013): 363-368.

[3]. Kani, Ernst. "The State Of The Art Of Elliptic Curve Cryptography." Queen's University.

[4]. Kapoor, Vivek, Vivek Sonny Abraham, and Ramesh Singh. "Elliptic curve cryptography." Ubiquity 2008.May (2008): 7

[5]. Aditya Birla, Alfred Menezes, and Scott Vanstone."The state of elliptic curve cryptography." Towards a quarter-century of public key cryptography.Springer US, 2010.103-123.

[6]. Wang, Hao dong, Bo Sheng, and Qun Li. "Elliptic curve cryptography-based access control in sensor networks." International Journal of Security and Networks 1.3-4 (2006): 127-137.

[7]. Ikshwansu Nautiyalet.al,"Encryption using Elliptic Curve Cryptography using Java as Implementation tool", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 1, January 2014.

[8]. Bos, Joppe W., et al. "Elliptic curve cryptography in practice." Financial Cryptography and Data Security.Springer Berlin Heidelberg, 2014.157-175.

[9]. Käsper, Emilia. "Fast elliptic curve cryptography in OpenSSL." Financial Cryptography and Data Security.Springer Berlin Heidelberg, 2011. 27-39

[10]. Amara, Moncef, and Amar Siad."Elliptic Curve Cryptography and its applications." Systems, Signal Processing and their Applications (WOSSPA), 2011 7th International Workshop on. IEEE, 2011.

[11]. Sinha, Rounak, Hemant Kumar Srivastava, and Sumita Gupta. "Performance based comparison study of RSA and elliptic curve cryptography."International Journal of Scientific & Engineering Research 4, no. 5 (2013): 720-725.