**National Institute Of Technology, Hamirpur (H.P)**

**Innovative Research Incubation Club**

**Innovative Research Project Proposal/Format**

**Research Project Title**

Diffie-Hellmann Key Exchange with Elliptic Curves (ECC) and Advanced Encryption Standard (AES) Based Security Framework for Internet of Things and Cloud Computing

**Project Description**

**Abstract:** The Internet of Things is integrating information systems, places, users andBillions of constrained devices into one global network. This network requires secure and private means of communications.. We present Diffie-Hellman key exchange with elliptic curves and AES Cryptosystems which address the security issues in the heterogeneous IoT networks. The security strengths of various public key cryptosystems are analysed and ensured ECC is one of the best cryptosystems for internet of things and cloud.

**Keywords:** ECC, RSA, AES, IoT, Cloud Computing, Security, Smart Environment

**1. Introduction**

Internet of Things (IoT) and Cloud Computing play a vital role in the field of Information Technology [1]. Internet of things is not a single technology, it is the concept in which many of the new things are getting networked and connected anytime, anyplace with anything and anyone ideally using any path or network and any service in a heterogeneous environment [2]. European Research Cluster on the Internet of Things (IERC) states that “Internet of Things is a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual things have identities, physical attributes and virtual personalities and use intelligent interface and are seamlessly integrated into the information network”[3].

In a nutshell, IoT is characterized by the real world of smart objects with limited storage and processing power [4]. In contrast, Cloud Computing is characterized by virtual world with unlimited capability in terms of storage and processing power.

Though the IoT and Cloud Computing have emerged as independent technologies, merging these two have augmented the field of future networks. Internet of Things is enhanced by the unlimited capabilities and resources of cloud to compensate its technological constraints such as storage and processing. On the other hand, cloud has extended its scope to the real world through IoT in a more dynamic and distributed way to deliver new applications and services in a real time scenario at large scale. Consequently, the integration of IoT and Cloud, the complementary technologies enhance the smart environment to reach the heights of availing any services and applications anywhere, anytime, any firm and any device irrespective of any underlying technology [7].

1

**2. Motivation**

Taking into account the relatively high computing resources required to compute discrete logarithms, elliptic curve crypto systems allow to significantly reduce size of the encryption keys. The small key size enables faster execution of various cryptographic operations. According to the literature, it is concluded that RSA key generation takes place substantially slower than elliptic curve based crypto systems of comparable level of security. The results are listed on the table below:

For the same security level ECC requires less no of bits as compared to RSA. Thus for devices in internet of things having limited resources like processing power, battery, memory ECC will be the good choice. Computation in ECC takes less time and hence it is fast. Keys generated by ECC can be used by the AES, 3DES cryptosystems for encryption and decryption purposes.

Some of the benefits of ECC are:

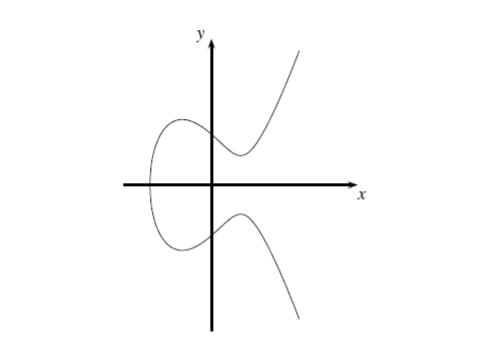
1. **Key size:** The key of an elliptic curve based crypto system takes significantly lessmemory. The ratio increases rapidly with the increase of security levels. For instance, RSA crypto system with the key length of 1024 bits, is equivalent to an elliptic curve crypto system with the key length of 163 bits.
2. **Cryptographic operations performance:** Thanks to the smaller size of keys, thecryptographic operations such as key and digital signature generation are carried out significantly faster. For instance, an elliptic curve crypto system with the key length of 233 bits corresponds to RSA crypto system with the key length of 2240 bits. In the first case the key is generated approximately 40 times faster.
3. **Resource saving:** Due to the smaller key sizes, algorithms of an elliptic curve basedcrypto systems can be executed on very limited resources.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Algorithm** | **Cryptosystems** |  | **Security level (bit)** | |  |
| **Family** |  |  |  |  |  |
|  |  | **80** | **128** | **192** | **256** |
|  |  |  |  |  |  |
| Integer | RSA | 1024 bit | 3072 bit | 7680 bit | 15360 bit |
| factorization |  |  |  |  |  |
|  |  |  |  |  |  |
| Discrete | DH,DSA, Elgamal | 1024 bit | 3072 bit | 7680 bit | 15360 bit |
| logarithm |  |  |  |  |  |
|  |  |  |  |  |  |
| Elliptic curves | ECDH, ECDSA | 160 bit | 256 bit | 384 bit | 512 bit |
|  |  |  |  |  |  |
| Symmetric-key | AES, 3DES | 80 bit | 128 bit | 192 bit | 356 bit |
|  |  |  |  |  |  |

**Table: 1** Comparison of different members of cryptosystems.

**3. ECC and AES based Security Framework**

**3.1 Definition of Elliptic Curves**



**Figure: 1** Example of Elliptic Curve ( ) over R [13]

**3.2 Group Operations on Elliptic Curves**

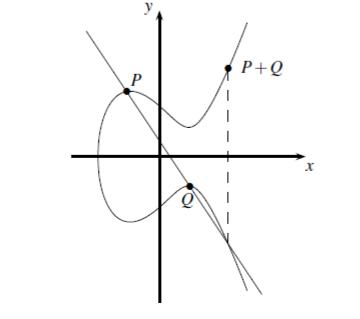
Let’s denote the group operation with the addition symbol “+”. “Addition” means that given two points and their coordinates, say P = (x1, y1) and Q = (x2, y2), we have to compute the coordinates of a third point R such that:

…(3)

There is a nice geometric interpretation of the addition operation if we consider a curve defined over the real numbers. For this geometric interpretation, we have to distinguish two cases: the addition of two distinct points (named point addition) and the addition of one point to itself (named point doubling).

**3.2.1 Point Addition P+Q**

This is the case where we compute R = P+Q and P Q. The construction works as follows: Draw a line through P and Q and obtain a third point of intersection between the elliptic curve and the line. Mirror this third intersection point along the x-axis. This mirrored point is, by definition, the point Figure 2 shows the point addition on an elliptic curve over the real numbers.

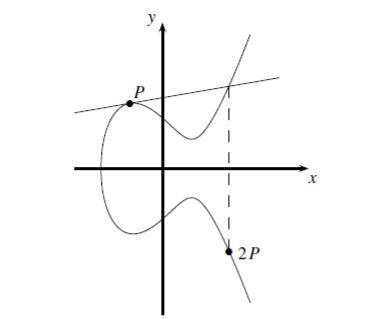


**Figure: 2** Point addition on an elliptic curve over the real numbers [13]

4

**3.2.1 Point Doubling P+P**

This is the case where we compute P+Q but P=Q. Hence, we can write R = P+P = 2P. We need a slightly different construction here. We draw the tangent line through P and obtain a second point of intersection between this line and the elliptic curve. We mirror the point of the second intersection along the x-axis. This mirrored point is the result R of the doubling. Figure 2 shows the doubling of a point on an elliptic curve over the real numbers.



**Figure: 3** Point doubling on an elliptic curve over the real numbers [13]

In a cryptosystem we cannot perform geometric constructions, so formulas for computation of points are given as

…(4)

…(5)

Where

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| s = |  |  |  | if P Q |
|  |  |  |
| = |  |  |  | if P=Q |
|  |  |  |

There exists an identity (or neutral) element O such that:

P + O = P

There exists an inverse of point such that:

P + (-P) = O

**3.3 Building a Discrete Logarithm Problem with Elliptic Curves**

**Theorem 1** The points on an elliptic curve together with O have cyclic subgroups. Undercertain conditions all points on an elliptic curve form a cyclic group.

**Theorem 2** Hasse’s theorem given an elliptic curve E modulo p, the number of points on

5

the curve is denoted by #E and is bounded by:

…(6)

**Elliptic Curved Discrete Logarithm Problem (ECDLP)**

Given is an elliptic curve E. We consider a primitive element P and another element T. The

DL problem is finding the integer d, where 1 ≤ d ≤ #E, such that:

…(7)

In cryptosystems, d is the private key which is an integer, while the public key T is a point on the curve with coordinates T = (xt, yt)

**3.4 Efficient Algorithm for Point Multiplication**

**Double-and-Add Algorithm for Point Multiplication**

Input: elliptic curve E together with an elliptic curve point P

Scalar d = Σi=0 t di 2i with di ∈ 0, 1 and dt = 1

Output: T = d.P

Initialization:

T = P

Algorithm:

**1** FOR i= t −1 DOWNTO 0

**1.1** T = T +T mod nIF di = 1

1.2 T = T +P mod n

**2** RETURN (T)

**3.5 Diffie–Hellman Key Exchange with Elliptic Curves**

**ECDH Domain Parameters**

1. Choose a prime p and the elliptic curve

E: …(8)

2. Choose a primitive element P = (xP, yP)

The prime p, the curve given by its coefficients a, b, and the primitive element P are the domain parameters.

**Proof**. Device1 computesa.B = a. (b.P)

While Device2 computes b.A = b. (a.P).

As can be seen in the protocol, Device1 and Device2 choose the private keys **a** and **b**, respectively, which are two large integers. With the private keys both generate their respective public keys A and B, which are points on the curve. The public keys are computed by point multiplication. The two parties exchange these public parameters with each other. The joint secret TAB is then computed by both Alice and Bob by performing a second point multiplication involving the public key they received and their own secret parameter. The joint secret TAB can be used to derive a session key, e.g., as input for the AES algorithm. One of the coordinates of the joint secret TAB can now be used as session key. In practice, often the x-coordinate is hashed and then used as a symmetric key.

**Security:**

The reason we are using elliptic curves is that the ECDLP has very good one-way characteristics. If an attacker Oscar wants to break the ECDH, he has the following information: E, p, P, A, and B. He wants to compute the joint secret between Device1 and Device2 TAB = a · b · P. This is called the elliptic curve Diffie–Hellman problem (ECDHP). There appears to be only one way to compute the ECDHP, namely to solve either of the discrete logarithm problems:

a = logP A Or

b = logP B

If the elliptic curve is chosen with care, the best known attacks against the ECDLP are considerably weaker than the best algorithms for solving the DL problem modulo p, and the

Best factoring algorithms which are used for RSA attacks. In particular, the index-calculus algorithms, which are powerful attacks against the DLP modulo p, are not applicable against elliptic curves. For carefully selected elliptic curves, the only remaining attacks are generic DL algorithms that is Shanks ‘baby-step giant-step method and Pollard’s rho method.

7

Since the number of steps required for such an attack is roughly equal to the square root of the group cardinality, a group order of at least 2160 should be used. According to Hasse’s theorem, this requires that the prime p used for the elliptic curve must be roughly 160-bit long. If we attack such a group with generic algorithms, we need around √2160 = 280 steps. A security level of 80 bit provides medium-term security. In practice, elliptic curve bit lengths up to 256 bit are commonly used, which provide security levels of up to 128 bit.

**4. Implementation in Software and Hardware**

In software, a highly optimized 256-bit ECC implementation on a 3-GHz, 64-bit CPU can take approximately 2 ms for one point multiplication. Slower throughputs due to smaller microprocessors or less optimized algorithms are common with performances in the range of 10 ms. For high-performance applications, e.g., for Internet servers that have to perform a large number of elliptic curve signatures per second, hardware implementations are desirable. The fastest implementations can compute a point multiplication in the range of 40 μs, while speeds of several 100μs are more common**.**

On the other side of the performance spectrum, ECC is the most attractive public key algorithm for lightweight applications such as RFID tags.

**References**

1. J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions, Future Generation Computer Systems, Vol.29, 2013, pp. 1645-1660.
2. O. Vermesan and P. Friess, Internet of Things from Research and Innovation to Market Deployment, River Publishers Series in Communications, Aalborg, 2014.
3. O. Vermesan and P. Friess, Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, River Publishers Series in Communications, Aalborg, 2013.
4. R. Roman, P. Najera and J. Lopez, Securing the Internet of Things, IEEE Computer, Vol.44, 2011, pp. 51-58. [5] L. Badger T. Grance, R.P. Corner and J. Voas, DRAFT Cloud Computing Synopsis and Recommendations, National Institute of Standards and Technology, 2011, pp. 84.
5. R. Buyya, J. Broberg and A. Goscinski, Cloud Computing Principles and Paradigms, WILEY, 2011.
6. C. Atkins, K. Koanagi, T. Tsuchiya, T. Miyosawa, H. Hirose and H. Sawano, A Cloud Service for End-User Participation Concerning the Internet of Things, Proceeding of IEEE Conference on Signal-Image Technology and Internet-Based Systems (SITIS), IEEE, 2013, pp. 273-278.
7. P. P. Pereira, J. Eliasson, R. Kyusakov, J. Delsing, A. Raayatinezhad, and M. Johansson,

Enabling Cloud Connectivity for Mobile Internet of Things Applications” Proceedings of

IEEE Symposium on Service Oriented System Engineering (SOSE), IEEE, 2013, pp. 518-526.

8

1. S. Aguzzi, D. Bradshaw, M. Canning, M. Cansfield, P. Carter, G. Cattaneo, S. Gusmeroli, G. Micheletti, D. Rotondi and R. Stevens, Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination. Final Report, European Commission, SMART 2013/0037, 2013.
2. N. Koblitz, Elliptic Curve Cryptosystems, Mathematics of Computation, Vol.49, pp. 203209, 1987.
3. V.S. Miller, Use of Elliptic Curves in Cryptography, Advances in Cryptology – CRYPTO’85, Lecture Notes in Computer Science, Springer Verlag, Vol.128,1985, pp. 417-426,
4. Moncef Amara and Amar Siad, Elliptic Curve Cryptography and its Applications, 7th International Workshop on Systems, Signal Processing and thir Applications (WOSSPA), IEEE, 2011, pp. 247-250.
5. Sandeep S. Kumar, Elliptc Curve Cryptography for Constrained Devices, PhD Thesis, Ruhur University Bochum, 2006.
6. Understanding Cryptography, A Textbook for Students and Practitioners by Paar, Christof, Pelzl

**Project Completion Time**

* Short term (up to one semester)

**Student Skills required, pre-requisites (If any):**

B. Tech. students of computer science and engineering with design, Analytical and problem solving capabilities

* Strong knowledge of Information Security
* Strong knowledge of Network programming
* Knowledge of Networking
* Good programming skills of JAVA, Python, NetBeans, Eclipse etc.

**Number of Students Required (UG/PG) for the Project:** Four

Dinesh Kumar, Nidhi Dhiman, Nishant Chaudhary, Shrirya Kaul (CSE Final Year).

**Name of Faculty Member:** Dr. Lokesh Chouhan

**Department:** COMPUTER SCIENCE AND ENGINEERING

**Email ID**: lokeshchouhan@gmail.com

**Contact No:** +91 8989624399

9