APPLICATION OF ELLIPTIC CURVE CRYPTOGRAPHY FOR MOBILE AND HANDHELD DEVICES

AJITHKUMAR VYASARAO[a1] AND K. SATYANARAYAN REDDY[b]

[a]Regional Research Centre VTU Belgaum
[b]Department of Information Science & Engineering, Cambridge Institute of Technology,

ABSTRACT

Voice communication becoming cheaper because of stiff competition among the service providers. Majority of the Internet Traffic consists of digitized voice and multimedia. Security is very much required for voice communication in order to safeguard privacy. Security always comes with premium such as computational power, memory and power.

KEYWORDS: Discrete Logarithm Problem, Elliptic Curve Cryptography, Point addition, Public Key Cryptography, Symmetric Key Cryptography, Voice Security.

Internet considered to be the most important invention of 20th century. Internet in one way or other way impacting our day to day transactions. Internet facilitates many applications such as Voice over IP, Internet Banking, Online shopping. All such applications are now being accessed using smart phones and hand-held devices. Internet applications are vulnerable to many attacks. There is a need for providing security to defend against such attacks.

VOIP SECURITY

Voice over IP technology deals with transmission of digitized voice data over Internet. Internet technology now being used extensively for communication, capable of transporting voice, data and multimedia traffic.

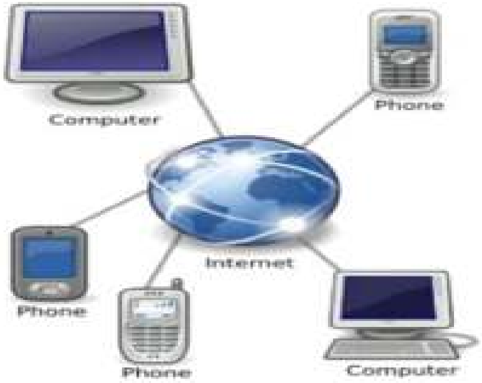

Figure 1: Voice Over IP

Voice over IP supports many combinations, one can place call from

i. Mobile phone to fixed line Phones.

ii. Mobile phone to anther mobile phone,

iii. Mobile phone to Personal Computer and

iv. Personal Computer to Personal Computer

This can lead to delay, jitter and packet loss, which in turn affect Quality of Service(QOS). Such issues can be addressed by proper QOS configuration on networking devices such as switch, router and gateway. Internet can pose lot of challenges for VOIP communication for various reasons. Data is transmitted without encryption over TCP/IP network. An attacker can launch attack without revealing his identity, personal and geographical as well. Voice data sent over Internet is vulnerable to all sorts of attacks such as spoofing, sniffing. By default, VOIP traffic over the Internet is sent in unencrypted form. This will open the door for Eavesdropping attack. Attacker can also launch DOS attack by flooding VOIP server with large number of inauthentic packets. Attacker can launch replay attack, such as spamming huge voice data to VOIP phones or voice mail box. Voice traffic composed of control traffic, signaling and media communications. Based on the protocols, VOIP communication can use single channel or multiple channels. Typically, these channels are Internet connections between two end points. Securing VOIP communication over IP network connections. Securing VOIP communication over IP network connections implemented in terms of authentication and encryption.

SECURITY PROTOCOLS

Security requirements can be categorized as

i. Confidentiality

ii. Integrity

iii. Authentication

[1]Corresponding author

Confidentiality can be assured by encrypting the data. An intruder will not be able to decrypt the data, without having access to the key for decrypting the data. Data Integrity can be implemented by adding some hash at the source and transmitted along with the data, at the receiving end. Data integrity is ensured if there is match between generated hash and received hash. Authentication ensures data is received from the right source. Cryptography which deals with encryption and decryption of data can be broadly classified into two major categories

i. Public Key Encryption or Asymmetric Key Encryption

ii. Symmetric Key Encryption

Public Crypto System uses key-pairs for encryption and decryption, whereas private crypto system uses same key for both encryption and decryption. Public Key crypto system uses more number of CPU cycles and memory. This requirement may not be suitable for mobile and hand-held devices as they are limited by computational power, memory and energy or battery power. Cryptographic algorithm should be energy efficient so that system can last for long time.

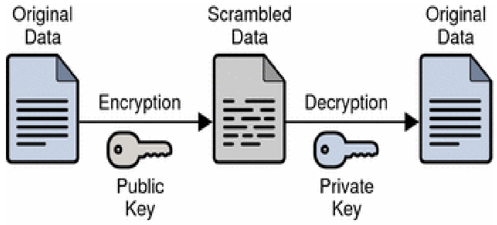

Figure 2: Public Key Encryption

Private key crypt system uses same key for encryption and decryption. Since same key is used for both encrypting the data and decrypting the data, this approach consumes less number of CPU resources compared to public key crypto system. The major challenge is how to exchange secret key over public infrastructure.

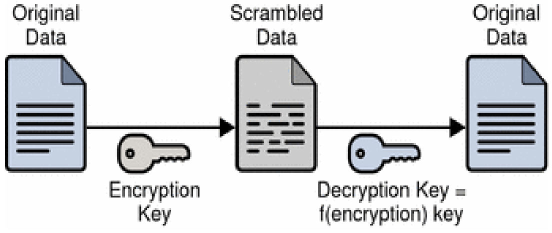

Figure 3: Symmetric Key Encryption

Modern cryptography uses combination of public and private key cryptosystem. Public key crypto system for key exchange and private key system for encryption and decryption. RSA which belongs to public key system is a good candidate, however RSA is not best candidate for mobile and handheld devices which have limited computational power and memory. Elliptic Curve Cryptography is a good candidate for mobile and handheld devices. We are proposing ECC for voice encryption, here we use ECC for key exchange and AES for encryption and decryption.

ELLIPTIC CURVE CRYPTOGRAPHY

ECC was discovered in 1985 by Neil Kibitz and Victor Miller. ECC schemes are public-key mechanisms that provide the same functionality of RSA. ECC belongs to public key cryptosystem category, which is based on Elliptic Curve Discrete Logarithm Problem for its security.

ECC is serving as an alternative to RSA by providing highest strength per-bit security compared to other prevalent cryptosystems existing today. ECC-160 provides security compared with RSA-1024 and ECC-224 provides security compared with RSA-2048 [Luma and Ameti, 2014]. Elliptic Curve Cryptography is such a powerful cryptosystem, which uses only 1/6 key size of RSA to guarantee the equivalent security [Park, 2016]. ECC uses shorter key lengths and provides security equivalent to RSA. This feature makes ECC very attractive for mobile hand-held devices.

Mathematical Background

An elliptic curve shown in Figure 4 can be represented as the set of solutions for the equation

y2=x3+ax+b(mod p) (1),

where a, b belongs Zp such that 4a3 +27b2 #0, including the point of infinity. Efficiency of elliptic curve algorithm is based on various factors like selecting the finite filed which could be either prime or binary, elliptic curve arithmetic such as point addition and point multiplication, scalar representation [Karthikeyan, 2012]. Algorithms are evaluated against two parameters such as time complexity and space complexity. An algorithm is considered to be complex if it takes more time to solve mathematical problem. The security of ECC is attributed to difficulty of solving discrete logarithm problem over the points on an elliptic curve, which is popularly known as Elliptic Curve Discrete Logarithm Problem (ECDLP). To give one example, the best-known method to solve ECDLP (pollard's rho algorithm) is fully exponential and substantially smaller key sizes as compared to other public cryptosystems to provide equivalent security [Kalra and Sood, 2011].

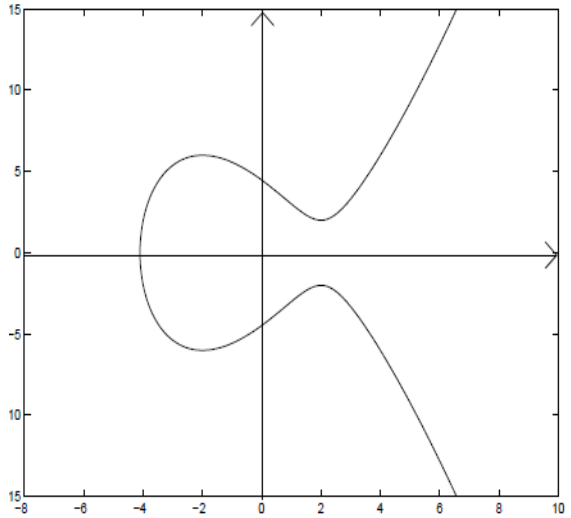

Figure 4: The Elliptic curve

The Elliptic Curve Discrete Logarithm Problem can be stated as follows. P and Q are two points on an elliptic curve and kP represents the point added to it self k times, where k is a scalar such that kP = Q. For a given P and Q, it is computationally infeasible to obtain k, if k is sufficiently large, k is the discrete logarithm of Q to the base P. ECC has certain characteristics that enables the process of taking any two points on a specific curve. Adding these 2 points results in another point on the same curve. There is inherent difficulty finding which 2 points have been used to arrive at the third point. This property is very much useful in cryptography [Ammayappan et. al., 2011]. Operations that are defined in elliptic curve cryptography are point addition which is shown in Figure 6, point multiplication and point doubling. Elliptic Curves have certain geometrical properties. Elliptic Curves symmetry over x-axis. If we take the reflection over the x-axis, we get another half of the elliptic curve. Point addition operation is defined over the elliptic curve. Take two points P and Q on the elliptic curve. Draw a line joining P and Q, extend this line so that it touches another point on the elliptic curve-R, now take the reflection of –R on the x axis that is R on the elliptic curve. Now R is the result of point addition P with Q.

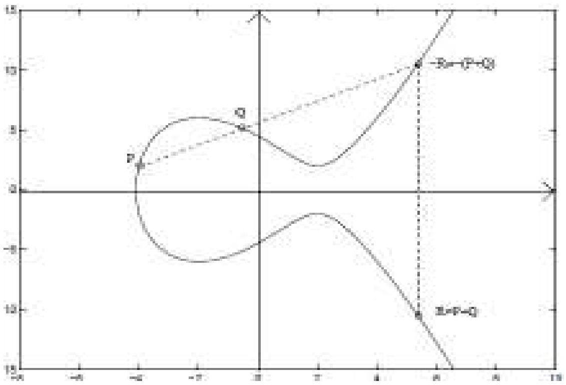

Figure 5: The Elliptic curve point addition

Another important operation defined in elliptic curve cryptography is point doubling. This can we considered as special case of point of addition where P=Q. Since we are going to add point P to itself, we don't have another distinct point on the elliptic curve to draw a line joining P to Q. In this scenario, a tangent to the elliptic curve is drawn keeping P as the starting. Tangent is extended and it intersects at another point which is considered to be –R, now take reflection on x-axis to obtain R. Now R=P+P = 2P, which is nothing but result of doubling of point P.

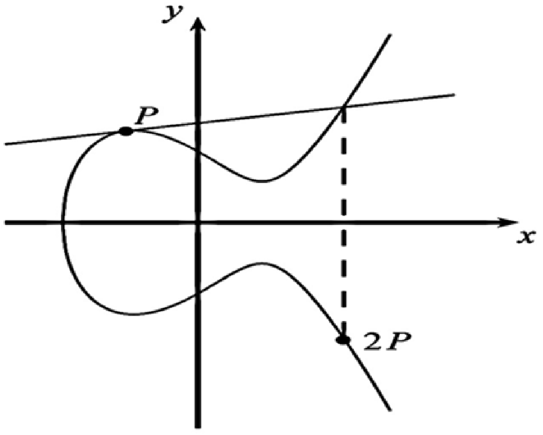

Figure 6: The Elliptic curve point doubling

Extending this point doubling operation, we can perform another operation, which is nothing but Elliptic curve point multiplication. Point multiplication is the operation of successively adding a point along an elliptic curve to itself repeatedly.

The Elliptic curve point multiplication is also referred as scalar multiplication, thus the most common name is elliptic curve scalar multiplication. Scalar multiplication is denoted as nP = P + P + … + P for some integer 'n 'and a point P = (x, y) that lies on the elliptic curve, E. There is one special case of point addition operation in elliptic curve. In this case point P is added to –P, which is nothing but reflection of point P on x-axis, when added P with –P by joining two points with a straight line, this resulting line will not intersect elliptic curve at another point, as this line is parallel to y-axis.

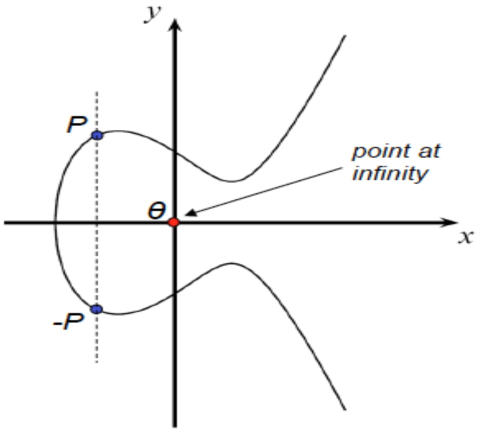

Figure 7: The Elliptic curve point addition special case

When point, P is added with –P the line intersects elliptic curve at the point of infinity, which is denoted as "θ". Point addition with point of infinity gives back to same point. In other words, $P + \theta = \theta + P = P$. Point of infinity serve as identity element with respect to group operation addition.

Elliptic Curve Discrete Logarithm Problem

Given a point P and Q is obtained by multiplying P by a scalar integer d. Given P and Q it is difficult to derive integer d. Adding d times P. In other words, $P + P + \ldots + P = dP = Q$. Choosing large d will make attacker job hard. If 'd' is known, we need efficient algorithm to compute dP. One such algorithm is double and add. Strength of any cryptographic algorithm is measured against hardness or effort required to break the key. Effort required to break the key is proportional to key length. In other words, 128-bit key provides higher security compared to 64-bit key. Advantage of using Elliptic Curve Cryptography is ECC provides better security with smaller key size compared to its other public key cryptographic algorithms like RSA. Elliptic Curve Cryptography can be used for exchanging the secret key, encryption and decryption of data. Diffie-Hellman proposed first key exchange protocol. A variant of Diffie-Hellman key exchange algorithm can be implemented using ECC.

KEY AGREEMENT

Key agreement protocols play very important role for ensuring secure communication over insecure network. In voice communication, unless and otherwise specified, it refers to communication between two entities. In this paper, we are referring only unicast voice communication scenario, excluding multicast and broadcast communication cases. A key establishment protocol allows two or more parties to establish a shared secret key for encrypted communication over unsecure network]. A two-party key agreement protocol facilitates establishment of common key between two communicating entities. Both entities contribute some information to generate the shared session key. Diffie-Hellman proposed first key agreement protocol, which is considered to be original break-through in public-key cryptography. However, Diffie-Hellman protocol is susceptible to man-in-the-middle attack as there is no mechanism to authenticate two entities participating in the secure communication. Basic requirement of key agreement protocol is to ensure session key is established only between the intended parties to the communication. The desirable characteristics of two-party key agreement protocol includes known key security, perfect forward secrecy, key compromise impersonation, unknown key share, implicit key authentication, key confirmation and explicit key authentication which needs to be satisfied while designing a protocol for efficacy [Ammayappan et. al., 2011].

ANALYSIS OF ELLIPTIC CURVE CRYPTOGRAPHY

Diffie-Hellman Key Exchange variant for ECC

Diffie-Hellman key exchange algorithm is used for exchanging the secret key over insecure channel. Let us take a scenario in which Alice and Bob two parties need to exchange secret key. Elliptic Curve Cryptography provides a way to exchange secret key.

i. Alice and Bob agree upon starting point P point on elliptic curve publicly defined $y2 = x3 - 4x + 0.67$

ii. Alice selects his private 'α' and computes αP shares this with bob

iii. Bob selects his private 'β' and computes βP shares with Alice

iv. Alice receives βP and computes $\beta P \alpha$ by multiplying with his private

v. Bob receives αP and computes αPβ by multiplying with his private

It is obvious βPα = αPβ, hence both Alice and Bob have same key which serves as private key for further encryption and decryption.

Security provided by ECC

ECC provides better security against attacks like factoring attacks. Given Q=dP, it is difficult to derive secret d for a given Q and P. There are some algorithms used to attack ECC such as Baby-Step Giant-Step and Pollard- Rho method.

Complexity of such methods are approximately √ p. An elliptic curve using a prime d with 160 bit approximately results in 2160 points, an attacker need at least 2^{80} steps on an average, another value for d with 256 bits generates 2256 points and provides security of 2^{128} steps on an average to break the system.

CONCLUSION

Elliptic Curve Cryptography finding new applications where computational power and memory are major factor. Elliptic Curve Cryptography can be used for efficient key exchange between the end points. Elliptic Curve Cryptography can also be used authenticating the end points in terms of digital signature Once has to choose the right Elliptic Curve to provide better performance and desired level of security based on the mobile and handheld device requirements. This work can be extended by choosing right curves for different VOIP end points and analyzing the performance, so that it can be fine-tuned.

REFERENCES

Luma A. and Ameti L. 2014. “ECC secured voice transmitter”. Proceedings of the World Congress on Engineering.

Park H.A., 2016. “Secure chip based encrypted search protocol in mobile office environments”. International Journal of Advanced Computer Research, **6**(24):72.

Karthikeyan E., 2012. “Survey of elliptic curve scalar multiplication algorithms”. International Journal of Advanced Networking and Applications, **4**(2):1581-90.

Kalra S. and Sood S.K., 2011. “Elliptic curve cryptography: Survey and its Security Applications”. In proceedings of the International Conference on Advances in Computing and Artificial Intelligence, pp. 102-106). ACM.

Ammayappan K., Negi A., Sastry V.N. and Das A.K., 2011. “An ECC-Based Two-Party Authenticated Key Agreement Protocol for Mobile Ad Hoc Networks”, Journal of Computers, **6**(11).