Review Article

ACCENTS Transactions on Information Security, Vol 2(6)
ISSN (Online): 2455-7196
http://dx.doi.org/10.19101/TIS.2017.26001

A survey on security of mobile handheld devices through elliptic curve cryptography

Ajithkumar V[1*] and K Satyanarayan Reddy[2]
Research Scholar RRC Belgaum, Software Engineer CISCO Systems[1]
Professor and Head of the Department Information Science & Engineering, Cambridge Institute of Technology, Bangalore[2]

Abstract
Mobile hand-held devices find their best suited for military application, due to ability to deliver real-time voice data. Military applications demand stringent requirements in terms of data confidentiality, authentication. Security can be provided using strong encryption. There are various parameters which need to be considered such as power consumption, execution time, QOS. In this paper, analysis is done regarding various existing available papers which discuss the implementation of security methods for handheld devices on certain parameters.

Keywords
Cryptographic algorithms, Discrete logarithm problem, Elliptic curve cryptography, RSA, Security.

1.Introduction
Cryptography is the science of constructing encryption and decryption algorithms. The term cryptography evolved from the Greek work kryptos which means secret writing. In other words cryptography is process of modifying the messages in such a way that is meaning is hidden and only can be reconstructed using decryption mechanism which does opposite to the encryption process. Encryption algorithms classified into two major categories. Symmetric Encryption: Symmetric encryption uses same key for encryption and decryption. The advantage with symmetric key encryption is that, uses less CPU resources, for encrypting and decrypting the data. Biggest challenge here is, how to exchange the key between communicating parties. Asymmetric Encryption: Asymmetric encryption uses key pairs for encryption and decryption. Asymmetric key encryption uses more CPU resources, since it uses different key for encryption and decryption. The beauty of asymmetric encryption, pair of key is generated at each communication end point, public key is shared and private key is retained. Public key is used for encryption and private key is used for decryption.

Cryptography is gaining more importance day by day. Now we are witnessing impact of Internet and Tele-Communication. World is moving towards complete digitization, we have new challenges of protecting the information from intruders. Now smart phones are becoming part and parcel of every body's life. Smart phones are becoming smarter, and hardly any difference between computer and mobile phones, in terms of computational power, variety of applications that can be used on mobile phones increasing beyond leap and bounds. Most of the financial transactions are being carried out using smart phones today. Mobile banking, on-line reservations, utility bill payments. Now people started using e-currency like Airtel Money[TM], Paytm[TM]. Every new application which uses Internet has to be protected. Hackers becoming more intelligent. There is race between people who try to protect the information and hackers. Latest addition is ransom wares.

Mobile and handheld devices have some limitations in terms of resources, such as CPU, memory. Encryption and decryption process consumes lot of CPU cycles. Hence, there is a need of developing encryption algorithms which can take care of these requirements. Encryption techniques using RSA ruled the world for almost 20 years. Now there is a paradigm shift, RSA has some overhead when it comes to mobile and hand held devices. Strength of

*Author for correspondence

the security algorithm depends on the key length, and more CPU and memory requirements with the increase in key length. Now there is a need for achieving higher security with limited computational resources. In this context Elliptic Curve Cryptography makes very big impact. ECC uses small key size and provides more security compared to its counterpart RSA.

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 [1]. Elliptic Curve Cryptography is such a powerful cryptosystem, which uses only 1/6 key size of RSA to guarantee the equivalent security [2].

Comparison of ECC and RSA shown in *Table 1* gives an idea about strength of ECC.

Table 1 Comparison of RSA with ECC

RSA	ECC
512 bits	106 bits
768 bits	132 bits
1024 bits	160 bits
2048 bits	224 bits

ECC uses shorter key lengths and provides security equivalent to RSA. This feature makes ECC very attractive for mobile hand-held devices.

2.Mathematical background

An elliptic curve shown in *Figure 1* can be represented as the set of solutions for the equation

$$y2=x3=+ax+b(\text{mod } p) \quad (1)$$

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 [3]. Algorithms are evaluated against two parameters such as time complexity and space complexity. An algorithm is considered to be complex if it take 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 [4].

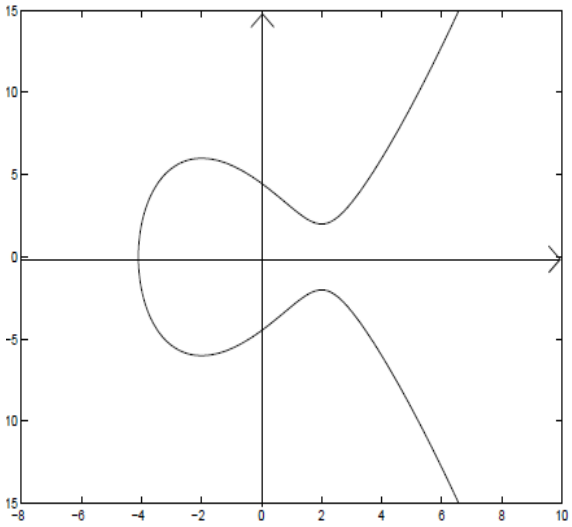

Figure 1 Elliptic curve

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 [5].

Operations that are defined in elliptic curve cryptography are point addition which is shown in *Figure 2*, 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 other 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.

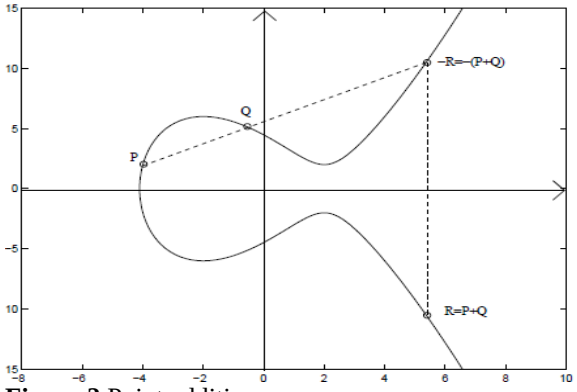

Figure 2 Point addition

3.Applications of ECC

A. ECC for mobile devices

The difference between computer and mobile devices are withering away day by day. Now a day's one can use mobile phone as a computer and perform basic operations like accessing the internet, sending and receiving mails. Now day's corporate companies provide chat and audio conferencing applications using which employees can join meetings and carry out day to day work. Most of the commercial transactions like money transfer, utility bill payments, on-line shopping are supported on mobile devices. Hence there is a huge security risk. Mobile devices can use traditional symmetric key crypto system for securing the transaction; however the biggest challenge is how to transfer the secret key over the public infrastructure which is vulnerable to eve dropping. Hence public key crypto system is preferred choice. Public key crypto system demands resources like CPU and memory, which is the limiting factor. Elliptic Curve Cryptography plays very important role here, since it provides greater security using smaller keys.

B. ECC for VOIP

Voice over IP is very prominent technology. Securing voice communication is need of the day. Now many VOIP products are supporting encryption. ECC is already being used for voice encryption.

C. Smart cards

Smart cards resembles credit card in shape and size. Smart cards have microchip, which is integrated into them. Smart cards equipped with a CPU, memory, Input and Output peripherals. In other terms they are like secure portable microcomputers [6]. Smart cards are having wide variety of applications. Smart cards can be used as debit or credit cards, personal identification cards. These qualities of the smart cards demand security requirements. Hence ECC can be used to provide security for transactions carried out using smart card [7].

D. PDAs

A personal digital assistant (PDA), also known as a palmtop computer, or personal data assistant, is a mobile device that functions as a personal information manager. Nearly all current PDAs have the ability to connect to the Internet. A PDA has an electronic visual display, enabling it to include a web browser, all current models also have audio capabilities enabling use as a portable media player, and also enabling most of them to be used as mobile phones. PDAs have more computing power compared to mobile devices like cell phones; however, PDAs do not have sufficient bandwidth, which mandates them to use light weight protocols for implementing the security. In these scenarios ECC will be preferred choice over any other public key system. Already many companies working in this direction, so that security can be provided to PDAs and hand-held devices using ECC. Good number of publication shows recent trends. ECC is gaining lot of importance and lot of research is happening in this area. Protocol based on ECC for mobile devices and ECC for smart cards shown in *Table 2* and *Table 3*

Table 2 Protocol based on ECC for mobile devices

Year	Protocol
2010	An Asymmetric Authentication Protocol for Mobile Devices Using Elliptic Curve Cryptography[8]
2014	Secure Mutual Authentication Protocol[9]
2014	An Asymmetric Authentication Protocol for Mobile Hand held Devices using ECC over Point Multiplication Method[10]

Table 3 Protocol Based on ECC for smart cards

Year	Protocol
2010	Timestamp Based Authentication Protocol for Smart Card Using ECC[11]
2014	Efficient password-authenticated key agreement protocol for smart cards based on ECC[12]
2014	A Secure Biometrics-Based Multi-Server Authentication Protocol Using Smart Cards[13]

4.Related work

There is always some trade-off trying to achieve security using existing resources. In [14] analysis is done regarding video decoding on mobile handheld devices. It has been shown that increasing resolution

needs to pay higher price in energy consumption than justified. Whereas, increasing bit rate gives a better picture quality without inducing too much energy consumption. So, handheld device users are encouraged to use higher bit rate to encode films if better picture quality is required. This clearly shows that encryption algorithm should take care of power consumption as one of the parameter. It has been shown in [15] point multiplication using divide and conquer reduces the number of clock pulses and power consumption and it also increases the performance of ECC. In [16], analysis is done regarding issues in ECC implementation for constrained environment such as hand-held mobile devices. Implementing ECC entirely in hardware can prove to be cheaper and faster, but it lacks the flexibility with respect to algorithms and parameters. This could increase development cost to support multiple algorithms.

5.Conclusion

We are witnessing era of internet of things (IOT), where security is prime focus and achieving higher security using less resources is need of the hour. RSA ruled the world for almost 40 years, but security requirements are changing, security is required for devices with lesser computational power such as PDAs and mobile devices. In this context elliptic curve cryptography plays pivotal role. Analysis shows that when devising an efficient ECC algorithm for mobile handheld devices various parameters such as power consumption, memory and CPU cycles, quality of service for voice should be taken into consideration. Some requirements are very stringent, but we need to optimize at the algorithm level. Hardware implementation seems to be attractive but results in higher development cost due to the lack of flexibility.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Luma A, Ameti L. ECC secured voice transmitter. In proceedings of the world congress on engineering 2014.

[2] Park HA. Secure chip based encrypted search protocol in mobile office environments. International Journal of Advanced Computer Research. 2016; 6(24):72.

[3] Karthikeyan E. Survey of elliptic curve scalar multiplication algorithms. International Journal of Advanced Networking and Applications. 2012; 4(02):1581-90.

[4] Kalra S, Sood SK. Elliptic curve cryptography: survey and its security applications. In proceedings of the international conference on advances in computing and artificial intelligence 2011 (pp. 102-6). ACM.

[5] Kumar KS, Sukumar R, Banu PA. An experimental study on energy consumption of cryptographic algorithms for mobile hand-held devices. International Journal of Computer Applications. 2012; 40(1):1-7.

[6] Berta IZ, Mann Z. Implementing elliptic curve cryptography on PC and smart card. Periodica Polytechnica, Electrical Engineering. 2002; 46(1):47-73.

[7] Verma SK, Ojha DB. A discussion on elliptic curve cryptography and its applications. International Journal of Computer Science Issues. 2012; 9(1): 74-7.

[8] Tiwari R, Sinhal A. Block based text data partition with RC4 encryption for text data security. International Journal of Advanced Computer Research. 2016; 6(24):107.

[9] Singhai P, Shrivastava A. An efficient Image Security mechanism based on Advanced Encryption Standard. International Journal of Advanced Technology and Engineering Exploration. 2015; 2(13):175.

[10] Nakhate MS, Goudar MR. Secure mutual authentication protocol. 2014; 4(3): 409-15.

[11] Chatterjee K, De A, Gupta D. Timestamp based authentication protocol for smart card using ECC. In international conference on web information systems and mining 2011 (pp. 368-75). Springer Berlin Heidelberg.

[12] Kalra S, Sood S. Efficient password–authenticated key agreement protocol for smart cards based on ECC. International Journal of Multimedia Intelligence and Security. 2013; 3(1):80-92.

[13] Odelu V, Das AK, Goswami A. A secure biometrics-based multi-server authentication protocol using smart cards. IEEE Transactions on Information Forensics and Security. 2015; 10(9):1953-66.

[14] Lin CH, Liu JC, Liao CW. Energy analysis of multimedia video decoding on mobile handheld devices. Computer Standards & Interfaces. 2010; 32(1):10-7.

[15] Sakthivel A, Nedunchezhian R. Analyzing the point multiplication operation of elliptic curve cryptosystem over prime field for parallel processing. International Arab Journal of Information Technology. 2014; 11(4):322-8.

[16] Paryasto MW, Kuspriyanto SS, Sasongko A. Issues in elliptic curve cryptography implementation. Internetworking Indonesia. 2009; 1(1):29-33.

This paper is selected from proceedings of National Workshop on Cryptology-NWC 2016 organized at JNN College of Engineering Shimoga, Karnataka, India during 11-13, August 2016.