Elliptic Curve Cryptography: An Overview

Zahoor Ahmad Dar

Research Scholar, (Computer Science) CMJ University, Shillong, Meghalaya

Abstract— Elliptic curve cryptography is one of the emerging techniques that stand as an alternative for conventional public key cryptography. Elliptic curve cryptography has several applications of which smart cards are also one among them. A smart card is nothing but a single chip that contains microprocessor components. Smart cards are mainly used for secured sign-on in big organizations. The security feature of smart card is provided by elliptic curve cryptography. Elliptic curve cryptography for smart cards can be implemented through several ways. Of them implementation using Galois Field is one of the very famous techniques. This essay discusses in detail how elliptic curve cryptography is implemented in smart cards using a concept called Galois finite field.

Index Terms — Elliptic curve cryptography, Cryptography.

----------♦----------

I. AN OVERVIEW OF ELLIPTIC CURVE THEORY:

Elliptic curves are referred so because they are explained by triple equations, similar to those used in the calculations of ellipsis (Silverman, 2009). The elliptic curve equation general form is:

b2 + cab + db = a3 + ea2 + fa + g

The below figure shows an example of ECC curve:

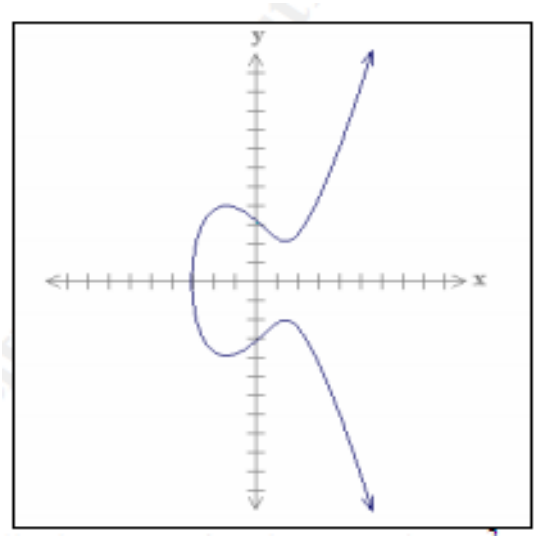

Figure 2: ECC Example

Source: sans.org

WHAT IS ELLIPTIC CURVE CRYPTOGRAPHY?

Elliptic curve cryptography was introduced by Neal Kolbitz and V Miller in 1985. Elliptic Curve Cryptography proposed as an alternative to established public key systems such as RSA and has recently achieved lot of attention in academia and industry (Pachgare, 2009, p 154). The major cause for the elliptic curve cryptography attractiveness is the fact that there is no sub exponential algorithm known to solve the discrete logarithm issue on an appropriately selected elliptic curve. This means that importantly smaller parameters can be used in Elliptic Curve Cryptography than in other competitive systems such as DSA and RSA but with similar security levels. Some advantages of having little key sizes include reductions and quicker computations in storage space, bandwidth and processing power. This makes Elliptic curve cryptography for constrained building of elliptic curve cryptography. Such as Personal digital assistants, pagers, smart cards and cellular phones. On the other hand the elliptic curve cryptography implementation needs many options such as the kind of the underlying finite field, algorithms for establishing the finite field arithmetic and so on.

Contrary to that Tilborg and Jajodia (2011, p 397) defined that elliptic curve cryptography enhances the analysis and configuration of public key cryptographic schemes that can be established using elliptic curves. The elliptic curve scheme analogues based on the discrete logarithm issue where the underlying group is the collection of points on an elliptic curve defined over a finite field.

Stavroulakis and Stamp (2010, p 35) described that elliptic curve cryptography enhances using the group of points on an elliptic curve as the underlying number system for public key cryptography. There are two major causes for using elliptic curves as a basis for public key cryptosystems. The first reasons are that the elliptic curve based cryptosystems exists to offer better security than traditional cryptosystems for a given key size. One can take benefit of this fact is to develop security or to develop performance by lowering down the size of the key while keeping common security. The second cause is that the additional framework on an elliptic curve can be destructed to build cryptosystems with interesting features which are impossible or critical to gain in any other way.

Elliptic curves are algebraic structures that form a basic class of cryptographic primitives which depend on a mathematical hard issue. The elliptic curve discrete algorithms problem is based on the intractability of deriving a huge scalar after its multiplications with a given point on an elliptic curve Yalcin (2010, p 3-11).

According to Zheng and Lionel (2006, p 354) an alternative to RSA elliptic curve cryptography is another approach to public key cryptography. Elliptic curve cryptography is based on the property of elliptic curve in algebraic geometrics. The elliptic curve cryptography permits one to select a secret number as a private key which is then used to select a point on a non secret elliptic curve. A nice property of an elliptic curve is that it enhances both parties to compute a secret key solely based on its private key and other's public key.

II. WHAT IS SMART CARD?

Smart cards are perhaps some of the most vastly used electronic components in use nowadays (Mayes and Markantonakis, 2009) define that. The below figure shows the physical appearance of smart card:

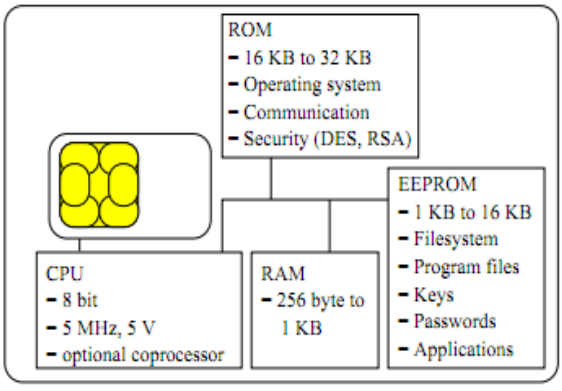

Figure 1: Physical Appearance of Smart Card

Source: Chen (2000), Java Card technology for Smart Cards: architecture and programmer's guide, Sun Microsystems Inc., USA, p 12

Because they have determined to be little and often concealed, smart cards have carried on their necessary works unnoticed largely but this situation is changing today. The high profile use of smart cards for IDs, credit cards, e-tickets and passports means that the smart card has now emerged as a common utility today. A smart card can be used in an automated electronic transaction. It is not easily copied or forged and it is used mainly to add security. Smart cards can also store data protectively and they can run or host a range of security functions and algorithms.

Contrary to that Cranor and Garfinkel (2005, p 229) defined that smart cards are praised always for their usability. They are mobile and they can be used in several applications and carry lesser administrative costs than systems based on several user name or passwords. On the other hand smart cards are also criticized for their less acceptance of market. Several people use this smart card added choice of security because readers and smart cards are not deployed vastly. However alternative form factors to the familiar plastic smart card are arousing, proponents of these technologies claims that they overcome the smart card limitations.

The smart card is a component which is able to store data and run commands. It is a single chip microcomputer with a size of 25 mm at most. This microcomputer is placed on a plastic card of the size of a standard credit card. Plastic cards have a long tradition. The smart card is a protective and tamper resistant component. The data stored on the card can be protected with a secret which is shared between the smart card and the cardholder. Only the person knowing the secret can use the card and the information stored on it. With the ability to execute commands and programs the smart card became able to decrypt and encrypt information argues, Hansmann (2002, pp 13-14).

Contrary to that Chen (2000, p 3) defined that a smart card processes and stores information through the electronic circuits fixed in silicon in the plastic substrate of its body. A smart card is a tamper resistant and portable computer. Unlike magnetic stripe cards, smart cards carry both information and processing power. Therefore they do not need access to remote databases at the transaction time.

According to American Heritage Dictionary (2006, p 292) a smart card is a small plastic card containing a computer chip. Several smart cards consist of memory chips to store data but several chips also contain microprocessors that

can process data. Smart cards are part of systems that enhance cardholders to buy services and goods, enter prohibited areas, links to cell phone networks or operate other operations that needs the processing and storage of recognizing information. SIM cards are a famous kind of smart card.

Beiske, Lee, Yim and Yu (2005, p 9) have defined that smart card is a credit card size plastic card which consists of magnetic data or microchip area. When this chip consists of monetary information which can be used for later transactions these smart cards belong to the group of electronic cash. Thus at present the electronic cash and smartcards are separated into online and offline applications. Some of the smartcard issues are that the smart cards are virtual and real stores accept them and are secure, efficient, speedy, paperless and intuitive. Smart card also supports several industries from banking to health care.

III. TYPES OF SMART CARDS

Smart cards fall into different groups. They can be categorized into microprocessor cards, memory cards, contactless cards and contact cards based on the variations in the access mechanism of cards. The types of smart cards are explained below:

A. Memory Cards:

The below figure shows the architecture of a memory card in block diagram form:

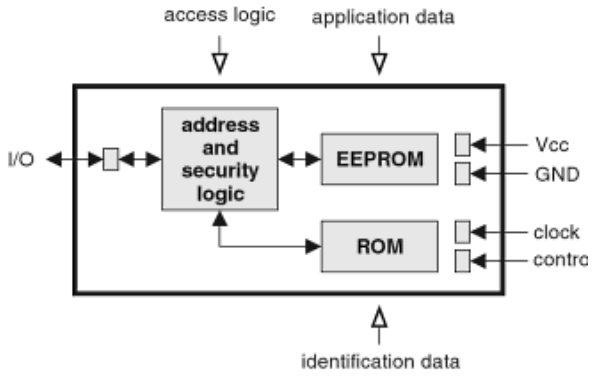

Figure 2: Memory card architecture

Source: Silabs.com

According to Ranki and Effing (2010, p 20) the required data by the application is stored in nonvolatile memory which is usually referred to as EEPROM. The memory access is controlled by the security logic which in the easiest case contains only of write security or erases security for the memory or specific memory regions. However there are also memory chips with more complex protective logic that can also perform easy encryption. The data is transferred to and from the card through a serial interface. The memory cards functionality is optimized usually for a specific application. Although this severely prohibits the cards flexibility it makes them quite costly. For memory cards typical applications are prepaid telephone cards and easy health insurance cards.

B. Microprocessor cards:

Microprocessor cards are sometimes known as microcontroller cards which consist of a microcontroller usually with mask Read Only Memory (ROM) and Electrically Erasable Programmable ROM (EEPROM) for personalization. Nowadays the microcontroller cards can have a technical capability to carry out several functions that are expected of a personal computer. These cards are assumed as truly smart and their processing ability that enhances them to be active and able to react and process to data in a given situation. The ability to perform independent calculations and to store several microprocessor cards applications means that they are suited well for application in transport, banking and some multi-application loyalty systems (Atkins, 2003, p 271).

C. Contact Cards:

The contact cards will be used as replacements for magnetic stripe cards mainly in access control and financial applications. Most of these contact cards will make their interface with the outside globe through a set of 6 to 8 contacts as defined in ISO 7816 part 1. The contact cards are themselves an important point of weakness in a smart card system: 1) The leads from the microcircuit to the contacts are of importance very thin and can become or break detached when the card is stressed or otherwise bent; 2) the contacts can become worn through damaged or excessive use by a defective reader or in a pocket; 3) they denote an obvious initiating point for any attack; and 4) In the reader the contact set is a mechanical component which can break or be damaged either maliciously or accidently (Hendry, 2001, p 88-89).

D. Contactless cards:

Jurgensen and Guthery (2002, p 34) described that a contactless card has an ICC embedded within the card. However it makes use of an electromagnetic signal to facilitate communication between the reader and the card. With these cards the important power to run the chip on the card id transformed at microwave frequencies from the reader into the card. The separation permitted between the card and the reader is quite small on the order of a few

millimeters. However this card provides a higher ease of use than cards that must be inserted into a reader. This ease of use can be mitigated by other factors.

IV. USE OF ELLIPTIC CURVE CRYPTOGRAPHY IN SMART CARDS

Tipton and Krause (2007, p 1064-1065) describe that ECC is suited ideally for implementation in smart cards for several reasons:

- **Scalability:** As the applications of smart card needs stronger and stronger security with big keys, Elliptic curve cryptography can continue to offer the security with proportionately lesser additional system resources. This means that with elliptic curve cryptography smart cards are capable of offering higher security levels without developing their prices.

- **Shorter transmission times and less memory:** The elliptic curve discrete logarithm problem algorithm strength means that strong security is gained with proportionately certificate sizes and smaller key. The smaller size of key in turn means that small memory is needed to store certificates and keys and that less data must be passed between the application and the card so transmission times are shorter.

- **No coprocessor:** The elliptic curve cryptography reduced processing times also make it separate for the platform of smart card. Other public key systems involve many computation that a dedicated hardware component referred to as crypto coprocessor is needed. The crypto coprocessors not only take up huge amount of space on the card but they also higher the price of the chip by about 20 to 30% which transforms to an increase of about $3 to #5 on the cost of each card. With elliptic curve cryptography the algorithm can be implemented in available Read Only Memory so no extra hardware is needed operate fast and strong functions of security.

- **On card key generation:** As described above the private key in a public key pair must be kept secret. To prevent the transaction truly from being refuted the private key must be inaccessible wholly to all parties except the entity to which it belongs. In applications using the other kinds of public key systems presently in use cards are personalized in a protective environment to meet this need. Because of the complexity of the computation needed generating keys on the card is typically impractical and inefficient.

With Elliptic Curve Cryptography the time required to produce a key pair is so small that even a component with a very limited computing smart card power can produce the key pair offered a better random number generator is possible. This means that the process of card personalization can be streamlined for applications in which no repudiation is necessary.

ELLIPTIC CURVE CRYPTOGRAPHY IMPLEMENTATION IN SMART CARDS

In general elliptic curve cryptography is implemented in smart cards by the use of a concept called finite field. Finite field is nothing but a set of elements which have a finite order. Galois Field represented by GF is a finite field whose order is in general a prime number, denoted as GF(m) or power of prime number denoted by GF (2m). The complexity of the arithmetic of the elliptic curve depends upon the finite field in which the elliptic curve is applied. GF(2m) is one of the most popular methods of implementing elliptic curve cryptography. The smart cards can be implemented using GF (2m). With GF (2m) a smart card is less costly because a coprocessor is not required. GF (2m) is referred to as a binary finite field or a two field characteristic. It can be looked as dimension's vector space k over the field GF (2m) that contains of 0 and 1 element. To describe in detail, there occur m elements (y0, y1, y2 . . . , ym-1) in GF (2m) such that every element y ε GF (2m) can be written distinctly in the form:

$$y = b0\ y0 + b1y1 \ldots + bm\text{-}1ym\text{-}1$$

where bi ε GF (2)

Such a set { y0, y1, y2 . . . , ym-1} is referred to as GF (2m) basis over GF (2). When such a basis is given a field element y can be denoted as a bit string (b0, b1 . . . bm-1). Performing extra field elements can be gained simply by XOR-ing bit-wise which are the elements vector representations. The rule of multiplication relies on the chosen basis. GF (2m) over GF (2) has several varied bases. Some bases may lead to several efficient arithmetic implementations in GF (2m) than other bases. The most famous 2 used bases are the normal and polynomial bases. In single representation of basis the elements can be transformed efficiently to other basis representation elements by using proper interoperability and change-of-basis matrix, between systems using 2 varied field types of representation can be gained easily. The equation of elliptic curve over GF (2m) is:

$$a2 + ya = a3 + by2 + c$$

where y, a, b, c ε GF (2m) and $c \neq 0$

The sum of 2 varied points on elliptic curve is evaluated as shown below:

(a1, b1) + (a2, b2) = (a3, b3); where a1≠a2

λ = (b2 + b1)/ (a2 + a1)

a3 = λ 2 + λ + a1 + a2 + c

b3 = λ (a1 + a3) + a3 + b1

On the elliptic curve the doubling a point is evaluated as shown below:

(a1, b1) + (a1, b1) = (a3, b3); where a1 ≠ 0

λ = a1 + (b1) / (a1)

a3 = λ 2 + λ + c

b3 = (a1)2 + (λ + 1) a3

Point compression permits the points on an elliptic curve additionally to be denoted with small amounts of data. In implementations of smart cards point compression is important because it lowers down not only the space of storage for keys on card, but also the huge number of data that requires to be transformed to and from the card. It can be accommodated with disregarded computation using GF (2m), but can cause implementations of GF (m) considerably. The hardware implementations of GF (2m) provide essential area size and performance benefits over hardware implementations of GF (m). Smart cards need several varied services of cryptographic with vastly fast performance may need coprocessors of cryptography. The coprocessor is configured to effective as possible GF (2m) may gain less space on the cost and smart card and may offer superior performance to an implementation of GF (m) (Stajano, 2007).

V. CONCLUSION

For smart cards elliptic curve cryptography is the most comfortable cryptosystem. Implementing smart cards using elliptic curve cryptography saves cost; time and area. Especially smart cards that are implemented over Galois field of order 2m, where m is a prime number, are very efficient in terms of performance as well as security. GF (m) and GF (2m) are the two extensive methods of implementation of smart cards currently in practice. However, with research being conducted in this area, to a great extent, there must be new methods of implementing Elliptic curve cryptography in the near future.

REFERENCES

- Silverman J H (2009), The arithmetic of Elliptic curves, Springer, Germany.
- Pachgare V K (2009), Cryptography and Information Security, PHI Learning Private Limited, New Delhi, p 154.
- Tilborg H C V A and Jajodia S (2011), Encyclopedia of Cryptography and Security, Springer, New York, p 397.
- Stavroulakis P and Stamp M (2010), Handbook of Information and Communication Security, Springer, Germany, p 35.
- Yalcin S B O (2010), Radio Frequency Identification: Security and Privacy Issues, Springer, Germany, p 3-11.
- Zheng P and Lionel M N (2006), Smart phone and next generation mobile computing, Morgan Kauffmann Publishers, UK, p 354.
- Mayes K E and Markantonakis K (2009), Smart cards, tokens, security and applications, Springer, Germany, p 1-2.
- Cranor L F and Garfinkel S (2005), Security and usability: designing secure systems that people can use, O'Reily Media Inc., USA, p 229.
- Hansmann U (2002), Smart card application development using Java: with 98 figures, 16 tables and a multi function smart card, Springer, Germany, p 13-14.
- Chen Z (2000), Java Card technology for Smart Cards: architecture and programmer's guide, Sun Microsystems Inc., USA, p 3.
- American Heritage Dictionary (2006), High definition: an A to Z guide to personal technology, Houghton Mifflin, USA, p 292.
- Beiske, Lee, Yim and Yu (2005), EOctopus in Hong Kong – A Feasibility Study, GRIN Verlag, Germany, p 9.
- Ranki W and Effing W (2010), Smart Card Handbook, John Wiley & Sons, UK, p 20.
- Atkins D (2003), The Smart Card Report, Elsevier, UK, p 271.
- Hendry M (2001), Smart card security and applications, Artech house, USA, p 88-89.

- Jurgensen T M and Guthery S B (2002), Smart cards: the developer's toolkit, Pearson Education, New Jersey, p 34.

- Tipton H F and Krause M (2007), Information Security Management Handbook, CRC Press, USA, p 1064-1065.

- Stajano F (2007), Security and privacy in ad-hoc and sensor networks, Springer,