A Survey of Elliptic Curve Cryptography Implementation Approaches for Efficient Smart Card Processing

Dr. Jayabhaskar Muthukuru[1] and Prof. Bachala Sathyanarayana[2]

[1] Sri Krishnadevaraya University

Received: 8 April 2012 Accepted: 4 May 2012 Published: 15 May 2012

Abstract

Smart cards have been used for many different purposes over the last two decades, from simple prepaid credit counter cards used in parking meters, to high security identity cards intended for national ID programs. This has increased data privacy and security requirements. Data protection and authentication is now demanded for performing Electronic payment and allow secure multi-level access to private information. ECC uses smaller key sizes compared to traditionally used RSA based cryptosystems. Elliptic Curve Cryptography is especially suited to smart card based message authentication because of its smaller memory and computational power requirements than public key cryptosystems. It is observed that the performance of ECC based approach is significantly better than RSA and DSA/DH based approaches because of the low memory and computational requirements, smaller key size, low power and timing consumptions.

Index terms— symbolic Elliptic Curve Cryptography, finite fields, smart cards, Biometrics.

1 I. INTRODUCTION

mart card is a credit-card sized plastic card with an embedded computer chip. Smart cards play an increasingly important role in everyday life. We encounter them as credit cards, loyalty cards, electronic purses, health cards, and as secure tokens for authentication or digital signatures. Their small size and the compatibility of their form make them ideal carriers of personal information such as secret keys, passwords, customization profiles, and medical emergency information. Electronic Payment is one of the most widely used applications of the smart card and is the most familiar among the average user. There are several different types of smart cards in this category, all of which deal with currency or a fiscal value. Smart cards can provide multi-factor authentication by using PIN/Biometrics combination with the card. verification and validation of a user identity using multiple authentication mechanisms. It often combines two or more authentication methods-for example, a three-factor authentication is based on password (Something you know), smart card (Something you have), and fingerprints (Something you are). For example, in addition to what the user knows (such as a PIN), the card can provide authentication using the card owner's digital certificate with the card owner's public key. The digital certificate associates the card owner's identity to the person's public key. The smart card also contains the card owner's private key, which can be used for digitally signing e-mail or documents. With the support of biometric technologies, the smart card can also be used to store biometric templates of the card owner, which can be used to verify the card owner by acquiring a biometric sample (such as a fingerprint) and matching it to the reference template stored on the card or off the card using a biometric authentication server. Using biometric templates can be considered for security-sensitive applications where PINs can be stolen [1]. Unlike standard public-key methods that operate over integer fields, the elliptic curve cryptosystems operate over points on an elliptic curve. Cryptographic algorithms based on discrete logarithm problem can be efficiently implemented using elliptic curves [21]. ECC is emerging as an attractive public-key cryptosystem for smart cards because compared to traditional cryptosystems like RSA/DH, it offers equivalent security with smaller key sizes, faster computation, lower power consumption, as well as memory and bandwidth savings [2].

2 II.

3 SMART CARD & ARCHITECTURE

Smart cards come in two varieties: memory and microprocessor. Memory cards simply store data and can be viewed as a small floppy disk with optional security. A microprocessor card, on the other hand, can add, delete and manipulate information in its memory on the card. Similar to a miniature computer, a

4 January 2012

Multi-factor authentication approach is recommended in which security requirements are intended for highly secure installation and mandate a robust solution. Multi-factor authentication ensures microprocessor card has an input/output port operating system and hard disk with built-in security features. a) Contact Vs. Contactless Smart cards have two different types of interfaces: contact and contactless. Contact smart cards are inserted into a smart card reader, making physical contact with the reader. However, contactless smart cards have an antenna embedded inside the card that enables communication with the reader without physical contact. A combi card combines the two features with a very high level of security.

5 b) Basic Smart Card Chip Architecture

The basic smart card architecture is shown on Figure 1. It is a complete set of a microcontroller. It is a small embedded computer with low processing power (8-bit CPU, 5 MHz clock) and small memory (4 Kb RAM, 16 Kb EEPROM, 64 Kb ROM).It is secure and inexpensive [20]. Test Logic: A verification function only used during the production process to test all internal circuits for manufacturing faults.

Security Logic: A continuous function that checks environmental conditions that could jeopardise the security of the smart card.

6 I/O Interface:

A communication function that takes care of receiving external commands and sending back responses using a serial communication protocol.

7 ROM:

The permanent memory of the chip. It can contain parts of the operating system and self test procedures.

8 RAM:

The CPU's scratch pad memory. This is used for storing temporary or intermediate data like session keys, internal variables and stack data.

EEPROM: Non-volatile updateable memory. It is used for storing application data like keys, PINs, balances, phone numbers, Biometric template and sometimes application or even operating system code.

Data Bus: The transfer channel within the chip. All information exchanged between the various functions passes through this channel.

9 III.

10 BIOMETRIC AUTHENTICATION

11 Biometric

technique is an automated methodology for the recognition of a person based on behavioral or physiological characteristics. These characteristics include features such as hand geometry, handwriting, face, fingerprints, vein, voice, retina, and iris. Biometric technologies are now the key to an extensive array of highly secured identification and personal verification solutions. Biometric system is a pattern recognition technology that makes personal identification of an individual by determining the authenticity of a specific physiological or behavioral characteristics possessed by the user [3].

12 a) Biometric Based Implementation on Smart Card

The use of biometrics within the card itself will mean that biometric features (fingerprint, retina, voice etc) can reliably identify a person. The use of some of these features has already been implemented in many applications. Table 1 below gives the required bytes for various biometric types. Additional information about biometric technology and standards can be found from the following organizations: The Biometric Consortium (www.biometrics.org), International Biometric Industry Association (www.ibia.rg), or BioAPI Consortium (www.iapi com) [4]. Match-off-card: For this type of implementation, the enrolled template is initially loaded onto the smart card and then transferred from the smart card via either contact or contactless interface when requested by the external biometric system. The external equipment then compares a new live template of the biometric with the one retrieved from the smart card. This implementation clearly has some security risks associated with transmitting the enrolled template off of the smart card for every biometric comparison. Appropriate security measures should be implemented to ensure the confidentiality and integrity of the released template.

Match-on-card: This implementation technique initially stores the enrolment template in the smart card's secure memory. When a biometric match is requested, the external equipment submits a new live template to the smart card. The smart card then performs the matching operation within its secure processor and securely communicates the result to the external equipment.

Biometric match-on-card approach can provide more private and secure identity verification system compare to match-off-card approach [5].

V.

13 ELLIPTIC CURVE ARITHMETIC

Elliptic curves are not like an ellipse or curve in shape. They look similar to doughnuts. Geometrically speaking they somehow resemble the shape of torus, which is the product of two circles when projected in three-dimensional coordinates. ECC makes use of elliptic curves in which the variables and coefficients are restricted to elements of a finite field. There are two families of elliptic curves defined for use in cryptography: prime curves defined over odd prime field F P and binary curves defined over Galois field GF (2 m). a) Geometrical Definition of Point Addition and point Doubling using chord-and-tangent rule

For any two points P(x 1 , y 1) ? Q(x 2 , y 2) on an elliptic curve, EC group law point addition can be defined geometrically (Figure **??**) as: "If we draw a line through P and Q, this line will intersect the elliptic curve at a third point (-R). The reflection of this point about x-axis, R(x 3 , y 3) is the addition of P and Q". Fig. **??** : Addition: R=P+Q For P=Q, point doubling, geometrically (Figure 3) if we draw a tangent line at point P, this line intersects elliptic curve at a point (-R). Then, R is the reflection of this point about x-axis. The dominant operation in ECC cryptographic schemes is point multiplication. This is the operation January 2012 which is the key to the use of elliptic curves for asymmetric cryptography—the critical operation which is itself fairly simple, but whose inverse (the elliptic curve discrete logarithm) is very difficult. ECC arranges itself so that when you wish to performance operation the cryptosystem should make easy encrypting a message with the public key, decrypting it with the private key the operation you are performing is point multiplication. Scalar multiplication of a point P by a scalar k as being performed by repeated point addition and point doubling for example 7P=(2((2P)+P)+P. c) Elliptic Curve Over F P and F 2 m Definition of elliptic curve over F P as follows [6].

Let p be a prime in F P and a, b? F P such that 4a 3 + 27b 2 ? 0 mod p in F P , then an elliptic curve E (F P) is defined as E (F P):= { p(x, y) , x, y ? F P } Such that y2 = x 3 + ax + b mod p together with a point O, called the point at infinity. Below is the definition of addition of points P and Q on the elliptic curve E (F P). Let P(x 1 , y 1) and Q(x 2 , y 2) then The point p(x, -y) is said to be the negation of p(x, y).

14 The elliptic curves over

y 2 ? y 1 If P ? ±Q (Point Addition) x 2 ? x 1 ? = 3x 1 2 + a If P = Q (Point Doubling) 2y 1 O If x 1 = x 2 and y 2 =? y 1 R = P+Q = Q = Q+P If P = O (x 3 , y 3) otherwise

Where? 2 +? + x 2 +x 1 + a If P ? ±Q (Point Addition) x 3 = ? 2 + ? + a If P = Q (Point Doubling) y 3 = ? (x 1 + x 3)+ x 3 + y 1 and y 2 + y 1 If P ? ±Q (Point Addition) x 2 + x 1 ? = x 1 x 1 If P = Q (Point Doubling) y 1

15 VI. ELLIPTIC CURVE CRYPTOGRAPHY FOR MESSAGE AUTHENTICATION

The use of Elliptic Curve Cryptography was initially suggested by Neal Koblitz [7] and Victor S. Miller [8]. Elliptic curve cryptosystems over finite field have some advantages like the key size can be much smaller compared to other cryptosystems like RSA, Diffie-Hellman since only exponential-time attack is known so far if the curve is carefully chosen [7] [6] and Elliptic Curve Cryptography relies on the difficulty of solving the Elliptic Curve Discrete Logarithm Problem ECDLP, which states that, "Given an elliptic curve E defined over a finite field F P , a point P?E (F P) of order n, and a point Q?E (F P) , find the integer k ? [0,n ?1] such that Q = k P. The integer k is called the discrete logarithm of Q to the base P, denoted k = log P Q".

16 a) Elliptic Curve Encryption/Decryption

Consider a message 'Pm' sent from A to B. 'A' chooses a random positive integer 'k', a private key 'n A ' and generates the public key P A = n A × G and produces the cipher text 'Cm' consisting of pair of points Cm = { kG , Pm + kP B } where G is the base point selected on the Elliptic Curve, P B = n B × G is the public key of B with private key 'n B '.

To decrypt the cipher text, B multiplies the 1st point in the pair by B's secret & subtracts the result from the 2nd point Pm + kP B -n B (kG) = Pm + k(n B G) -n B (kG) = Pm.

17 VII. VARIOUS ECC IMPLEMENTATION APPROACHES ON SMART CARD

In [14] Ahmad Khaled M. AL-Kayali demonstrated the advantages and disadvantages of using Prime/binary fields to implement ECC on smart cards. Prime fields are best for software applications where as Binary fields are suitable for Hardware applications **??**22]. To access remote information systems Password authenticated key agreement scheme [15] is very useful in limited computation and communication resource (smart card) environments. A two-phase authentication mechanism proposed [16] by Abhilasha, Anna Squicciarini, Elisa Bertino. In that first phase consists of a two-factor biometric authentication and second phase combines several authentication factors in conjunction with biometric to provide a strong authentication. A key advantage of this approach is that any unanticipated combination of factors can be used. Disadvantage of using existing remote user authentication schemes **??**17] [18] is if the smart card is lost and password is revealed then any one can impersonate to sever as authorized user. To overcome this K K Goyal and M S Chahar proposed a new scheme [19] using Biometrics. 3 shows NIST guidelines on choosing computationally equivalent symmetric and public-key sizes [10]. ECC is the best suited in constrained environments. The advantages like speed and smaller keys or certificates are especially important in environments where at least one of the following resources is limited [9]: processing power, storage space, band width, or power consumption. This advantage is because its inverse operation gets harder, faster, against increasing key length than do the inverse operations in Diffie Hellman and RSA. Table **??** shows a comparison of the RSA and ECC cryptographic operations performed by an SSL server. Open SSL speed program is used to measure RSA decryption and ECDH operation for different key sizes (a minor enhancement was made for collecting RSA-1536 numbers). These micro-benchmarks highlight ECC's performance advantage over RSA for different security levels. ECC's performance advantage increases even faster than its key-size advantage as security needs increase [10]. [1] [2] [3]

1

Figure 1: Fig. 1 :

[1] January 2012© 2012 Global Journals Inc. (US)

[2] © 2012 Global Journals Inc. (US) Global Journal of Computer Science and Technology Volume XII Issue I Version I

[3] January 2012© 2012 Global Journals Inc. (US) VIII.

3

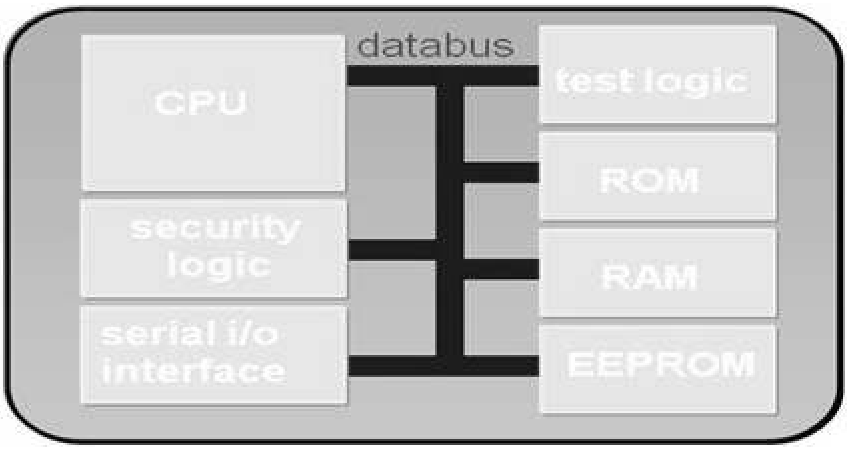

Figure 2: Fig. 3 :

222

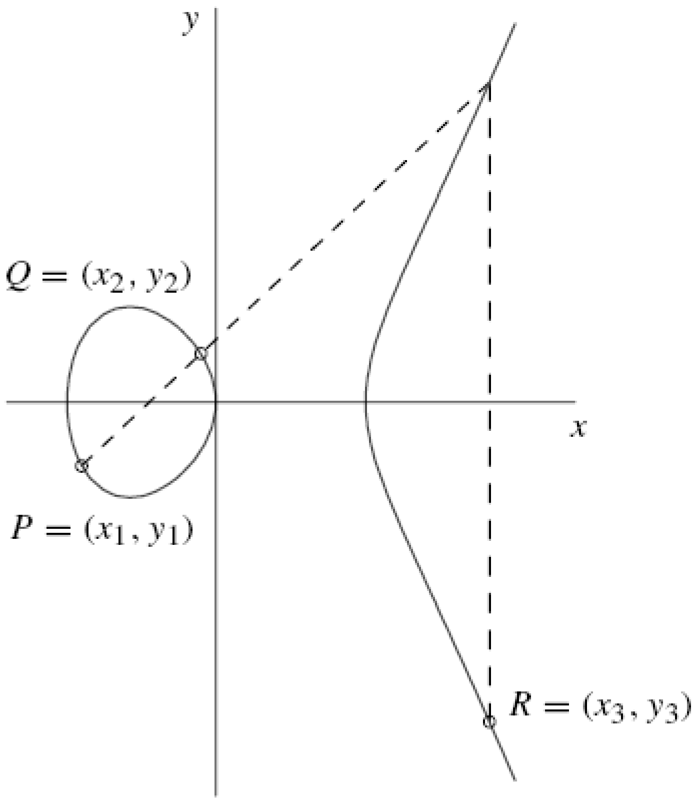

Figure 3: F 2 m 2 m)? 2 ?

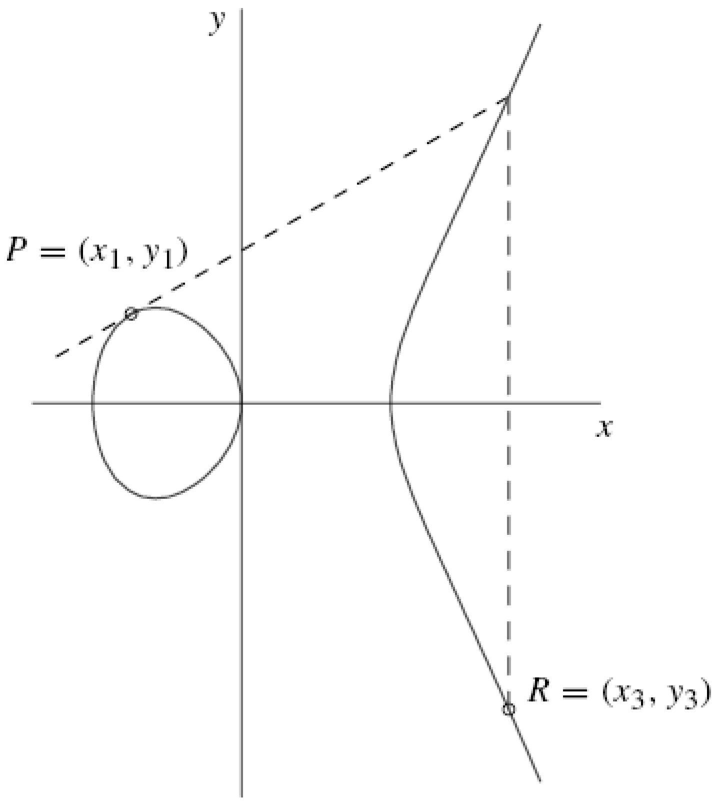

Figure 4:

1

systems

Biometric System	No. of Bytes Required
Finger scan	300-1200
Finger geometry	14
Hand geometry	9
Iris recognition	512
Voice verification	1500
Face recognition	500-1000
Signature verification	500-1000
Retina recognition	96

b) Classification of Biometric Approaches

Main Biometrics based smart card implementation approaches are "match-off-card" and "match-on-card".

Figure 5: Table 1 :

2

January 2012

Figure 6: Table 2 :

3

Security(bits)	RSA key Length (bits)	ECC key Length (bits)	DSA/DH (bits)	Key Size Ratio of RSA and ECC	MIPS years to attack	Protection attack
80	1024	160-223	1024	1:6	10 12	Until 2010
112	2048	224-255	2048	1:9	10 24	Until 2030
128	3072	256-383	3072	1:12	10 28	Beyond 2031
192	7860	384-511	7860	1:20	10 47	
256	15360	512+	15360	1:30	10 60	

Figure 7: Table 3 :

.1 CONCLUSION

The smart card market has experienced a spectacular growth over the past few years. Along with their growing popularity there has been a corresponding growth of interest in their security. With respect to endto-end security no other security solutions nearly as good and affordable as smart cards exist. Elliptic curve cryptography has been emerged as a vast field of interest for application specific security requirements. The elliptic curve discrete logarithm problem makes ECC most efficient compared to earlier RSA/DSA algorithms.

[Jena et al. ()] 'A Novel Remote User Authentication Scheme Using Smart Card based on ECDLP'. D Jena , S K Jena , D Mohanty , S K Panigrahy . *IEEE Proceeding of International Conference on Advanced Computer Control*, 2008.

[Goyal and Chahar (2011)] 'A Novel Remote User Authentication Scheme using Smart Card with Biometric Based on ECDLP'. K K Goyal , M S Chahar . *International Journal of Information Technology and Knowledge Management* July-December 2011. 4 (2) p. .

[Khalique et al. (2010)] *A Password-Authenticated Key Agreement Scheme Based on ECC Using Smart Cards*, Aqeel Khalique , Kuldip Singh , Sandeep Sood . May 2010. IJCA. 2.

[Caytiles (2011)] 'A Review of Smartcard Security Issues'. Hoon , Ronnie D Caytiles . *Journal of Security Engineering* Jun-2011. p. .

[Katiyar et al. (2010)] *A Survey on Elliptic Curve Cryptography for Pervasive Computing Environment*, Vivek Katiyar , Kamlesh Dutta , Syona Gupta . December 2010. IJCA. 11.

[Branovic et al. (2004)] *A Workload Characterization of Elliptic Curve Cryptography Methods in Embedded Environments*, R Branovic , E Giorgi , Martinelli . June-2004. ACM. 32.

[Opara et al. ()] 'Biometric and Systems Security: An Overview of End-To-End Security System'. Emmanuel Opara , Mohammad Rob , Vance Etnyre . *Communications of the IIMA* 2006. 6 (2) p. .

[Steel et al.] *Core Security Patterns: Best Practices and Strategies for J2EE?, Web Services, and Identity Management*, Christopher Steel , Ramesh Nagappan , Ray Lai . p. .

[Efficient and provably-secure identity-based signatures and signcryption from bilinear maps Proc. Of ASIACRYPT'05 ()] 'Efficient and provably-secure identity-based signatures and signcryption from bilinear maps'. *Proc. Of ASIACRYPT'05*, (Of ASIACRYPT'05) 2005. 3778 p. .

[Khaled and Al-Kayali ()] 'Elliptic Curve Cryptography and Smart Cards'. Ahmad Khaled , M Al-Kayali . *SANS Instutute*, 2004.

[Wasim and Al-Hamdani (2011)] *Elliptic Curve for Data protection*, A Wasim , Al-Hamdani . Oct-2011. p. . (Information Security Curriculum conference)

[Koblitz ()] 'EllipticCurve Cryptosystems'. N Koblitz . *Mathematics of Computation*, 1987. 48 p. .

[Hankerson et al.] *Guide to Elliptic Curve Cryptography*, Darrel Hankerson , Alfred Menezes , Scott Vanstone .

[Hitchcock et al. ()] 'Implementing an efficient elliptic curve cryptosystem over GF(p) on a smart card'. Yvonne Hitchcock , Edward Dawson , Andrew Clark , Paul Montague . *ANZIAM J* 2003. 44 p. .

[Zsolt and Adam ()] *Implimentating ECC on PC and smart card*, Istvan Zsolt , Berta , Zoltan Adam , Mann . `http://www.crysys.hu/publications/files/BertaM2002pp.pdf` 2002.

[Jena et al. (2009)] *Modified Remote User Authentication Scheme using Smart Card based on ECDLP*, Debasish Jena , Sanjay Saroj Kumar Panigrahy , Subhendu Kumar Jena , Kumar Pani . 2009, 28 -31 December 2009. Sri Lanka.

[Abhilasha et al. (2006)] 'Privacy Preserving Multi-Factor Authentication with Biometrics'. Anna Abhilasha , Elisa Squicciarini , Bertino . *DIM'06*, November 3, 2006.

[Smart Card Alliance white paper (2011)] *Smart Card Alliance white paper*, PAC-11002. March 2011. p. . (Smart Cards and Biometrics)

[Mohammed et al. (2004)] 'Smart Card Technology: Past, Present, and Future'. L Mohammed , Abdul Rahman Ramli , V Prakash , Mohamed B Daud . *International Journal of The Computer, the Internet and Management* January -April, 2004. 12 (1) p. .

[Gupta et al.] *Speeding up Secure Web Transactions using Elliptic Curve Cryptography (ECC)*, Vipul Gupta , Douglas Stebila , Stephen Fung , Sheueling Chang , Nils Gura , Hans Eberle . `http://www.isoc.org/isoc/conferences/ndss/04/proceedings/Papers/Gupta.pdf`

[Miller ()] 'Uses of Elliptic Curve in Cryptography'. V Miller . *Proceedings of Crypto'85, Lectures notes on Computer Sciences*, (Crypto'85, Lectures notes on Computer Sciences) 1986. Springer-Verlag. 218 p. . (Advances in Cryptography)

[Woodbury et al. ()] Adam D Woodbury , Daniel V Bailey , Christof Paar . *The Fourth Smart Card Research and Advanced Applications(CARDIS 2000) Conference*, September 20-22, 2000. (ECC on smart cards without coprocessors)