A Systematic Way to Provide Security for Digital Signature Using Elliptic Curve Cryptography

Prof Navneet Randhawa[1], **Er. Lolita Singh**[2]

Computer Science and Information Technology Department
Adesh College of Engineering and Technology, Faridkot, Punjab, India

Summary
E-Commerce [1] is an integral part of our lives now. It has boomed in popularity for both retailers and consumers and this trend is not going to stop anytime soon. The cost-benefits for businesses in overhead and the convenience for shoppers are strong motivators to continue the growth of e-commerce. While there are many benefits of e-Commerce, it is important to remember that there are definitive security challenges that businesses face in e-commerce. But, these are probably not enough to deter merchants (and customers) from engaging in online transactions; still they need to be paid careful attention in order to minimize the risk. Furthermore, E-Commerce is not only limited to a fixed computer it has become wire-free. In this paper the problem undertaken is"Security of Digital Signature in E-Commerce using Elliptic-Curve Cryptography".
E-Commerce security strategies deal with two issues: Protecting the integrity of the Business network and its internal systems and with accomplishing transaction security between the customer and the business. We use the concept of RSA (by Rivest, Shamir and Adleman.) and Elliptic Curve Algorithms to implement Digital Signature.

Keywords:
Digital signature, E-commerce, cryptography, security, public key algorithm: RSA, Elliptic curve;

1. Introduction

Rapidly rising cyber crime and the growing prospect of the Internet being used as a medium for terrorist attacks pose a major challenge for IT security. Cryptography is central to this challenge, since it underpins privacy, confidentiality, and identity, which together provide the fundamentals for trusted e-commerce and secure communications [17].
The main problem is to determine techniques, which ensure the confidentiality and privacy of message. Cryptography is one efficient way to ensure that if sent message fall into wrong hands, they cannot read it. It is the art of secret writing. In E-Commerce, Digital Signatures allow the verification of the 'origin' of messages (Transactions). We use the concept of RSA (by Rivest, Shamir and Adleman.) and Elliptic Curve Algorithms to implement Digital Signature. Our Problem is to find the equation of polynomial such that it is too complex to design its elliptic curve. An elliptic-curve group for cryptography comes from the multiples of a generating point G, a two-dimensional point on an elliptic curve over a finite field. In practice, the finite fields used are either integers modulo large primes, or a similar construction using 0/1 polynomials [15].
The Elliptic-Curve Digital Signature Algorithm (ECDSA) [19] is a Digital Signature Scheme based on ECC. Like all Digital Signatures, ECDSA is used for authentication and Integrity, but because it's based on ECC, its keys are smaller and its implementation is more efficient The crucial property of an elliptic curve is that we can define a rule for adding" two points which are on the curve, to obtain a 3rd point which is also on the curve. This addition rule satisfies the normal properties of addition. In math jargon, the points and the addition law form a finite Abelian group. The DSA scheme is another, pretty much any cryptographic scheme/protocol based on discrete logarithms can be easily converted to elliptic curve form. We have to use this property of Point addition to remove exponential calculations like in RSA and other public key algorithm. Because calculation of exponentials is most time consuming steps in mathematics. We study how to remove these complex operations? In this paper, first we practically implement the RSA algorithm in C language then we find out the complexity in the RSA calculations, and equations. So we will move on Elliptic-curve equations which are far easy and simple to implement and useful concept for the security of digital signature in E-commerce;

2. Related Work

Cryptography is a vital area in e-commerce security and is one of the fastest growing areas. It includes:

- Encryption algorithms
- Hash functions
- Digital signatures
- Digital certificates

We use various techniques to implement digital signature. Algorithm is used by a signatory to generate a digital signature on data and by a verifier to verify the authenticity of the signature. Each signatory has a public and private key. The private key is used in the signature

Manuscript received July 5, 2011
Manuscript revised July 20, 2011

generation process and the public key is used in the signature verification process. For both signature generation and verification, the data which is referred to a message,

2.1 Discrete Algorithms

Exponential Cipher:-

$$a^x = b \pmod p$$

Cryptosystem based on exponential congruences can be quite difficult to crack where for x. where a and b are known and p is prime.
Various algorithms based on the exponential congruence are: [14]

- Diffie-Hellman Key Exchange.
- Pohlig-Hellman exponential cipher
- The Elgmal Cipher
- The RSA Cipher
- The Elliptic Curve Approach

2.2 Pohlig-Hellman exponential cipher

This cipher is based on Fermats Little Theorem (FLT) is called Pohlig-Hellman exponential cipher
FLT: It state that if p be prime and b an integer such that p does not divide b. then $bp-1 \cong 1 \pmod p$.

2.3The Elgmal Cipher

Elgmal Cipher similar to Diffie-Hellman Key Exchange and Pohlig-Hellman in that breaking it require solving the discrete Logarithms Problem
1 The recipient of message must choose a large random safe prime p, and a generator g modulo p. p should be at least 1024 bits in length.
2. He select a random integer a such that $1<a<p-1$. And compute the least nonnegative residue r as

$$R \cong g^a \pmod p \quad (0<= r <p)$$

2.4 The RSA Cipher [15)

The RSA public key cryptosystem was invented by R. Rivest, A. Shamir and L.Adleman who invented it in 1977. The RSA cryptosystem is based on the dramatic difference between the ease of finding large primes and the difficulty of factoring the product of two large prime numbers (the integer factorization problem). This section gives a brief overview of the RSA algorithm for encrypting and decrypting messages.

3. Drawbacks of Existing system

- **Small Encryption exponent**:- To speed up encryption we use a small encryption exponent e.g.:- e =3 as their public key encryption key however a small value of e allows to compute the e^{th} root when same message is sent to multiple entities .
- **Require Higher Bandwidth**: for transmission also needs more circuitry devices.

4. Proposed Work

Although elliptic curves have been studied for over 150 years, they weren't applied to cryptography until very recently. In 1985, Neal Koblitz and Victor Miller independently proposed the use of elliptic curve points over a finite field for cryptosystems. Since then, several standards have accepted the use of elliptic curve cryptosystems.
Elliptic curve received the name from their relation to Elliptic Integral

$$\int_{z_1}^{z_2} \frac{dx}{\sqrt{x^3+ax+b}} \quad \text{and} \quad \int_{z_1}^{z_2} \frac{xdx}{\sqrt{x^3+ax+b}}$$

- Used in the computation of the arc length of ellipses.
- Elliptic curves are defined over fields
- We are interested in elliptic curves over finite fields such as prime $GF(p)$ or binary extension $GF(2^n)$ fields.
- Points on an elliptic curve (along with the point at infinity) over finite fields form an additive group.
- The operation is point addition given by addition law.
- The number of points on the curve is finite and countable.
- The point addition is closed, associative, etc.
- Group members are called (elliptic curve) points and represented by two coordinates $P = (x, y)$.

5. An Application of ECC ---ECDSA

5.1 A systematic approach of ECDSA

The elliptic curve digital signature algorithm is the elliptic curve analogue of DSA and serves the same purposes of key generation, signature generation, and signature verification. ECDSA was first proposed in 1992 by Scott Vanstone in response to NIST's proposal of DSS. It was later accepted in 1998 as an ISO standard (ISO 14888-3), as an ANSI standard (ANSI X9.62) in 1999, and as an IEEE standard (IEEE 1363-2000) and as a NIST standard (FIPS 186-2) in 2000.

5.2 Security of ECDSA

The generation of the public key in ECDSA involves computing the point, Q, where $Q = dP$. In order to crack the elliptic curve key, adversary Eve would have to discover the secret key d. Given that the order of the curve E is a prime number n, then computing d given dP and P would take roughly $2^{n/2}$ operations [1].

5.3 ECDSA Algorithm Approach

ECDSA is a very important application of ECC. As we know, digital signature is an important tool of authentication in E-business. It plays an important role in data integrity, non-repudiation and anonymity. In some sense, digital signature is more efficient than the traditional way, especially for long messages or documents. Because the traditional way can't assure that each page is unchanged. This algorithm is divided into 3 sub algorithm:-

5.3.1 Key Pair Generation Using ECDSA

Let A be the signatory for a message M. Entity A performs the following steps to generate a public and private key:

- Select an elliptic curve E defined over a finite field F_p such that the number of points in E (F_p) is divisible by a large prime n.
- Select a base point, P, of order n such that $P \in E(F_p)$
- Select a unique and unpredictable integer, d, in the interval [1, n-1]
- Compute $Q = dP$
- Sender A's private key is d
- Sender A's public key is the combination (E, P, n, Q)

5.3.2 Signature Generation Using ECDSA

Using A's private key, A generates the signature for message M using the following steps:
Select a unique and unpredictable integer k in the interval [1, n-1]

- Compute $kP = (x_1,y_1)$, where x_1 is an integer
- Compute $r = x_1 \bmod n$; If $r = 0$, then go to step 1
- Compute $h = H(M)$, where H is the Secure Hash Algorithm (SHA-1)
- Compute $s = k^{-1}\{h + dr\} \bmod n$; If $s = 0$, then go to step1
- The signature of A for message M is the integer pair (r,s)

5.3.3 Signature Verification Using ECDSA

The receiver B can verify the authenticity of A's signature (r, s) for message M by performing the following:

- Obtain signatory A's public key (E, P, n, Q)
- Verify that values r and s are in the interval [1,n-1]
- Compute $w = s^{-1} \bmod p$
- Compute $h = H(M)$, where H is the same secure hash algorithm used by A.
- Compute $u_1 = hw \bmod n$.
- Compute $u_2 = rw \bmod n$.
- Compute $u_1P + u_2Q = (x_0,y_0)$
- Compute $v = x_0 \bmod n$
- The signature for message M is verified only if $v = r$

6. Elliptic Curve Implementation Module

Step1: long int calad (long int*, long int*, long int*, long int*, long int*, long int*, long int, long int)
This module perform the addition of two elliptic curve points to generate third point., It accept parameters(x1,y1,x2,y2,x3,y3,a,p).
Return resultant point in pointer variable x3, y3.
Step 2: long int caldb (long int*, long int*, long int*, long int*, long int, long int)
This module performs the doubling operation on elliptic curve. This module takes elliptic point x1, y1 and store the result in x2, y2, a, p are passed as arguments.
Step3: calmod (long int, long int):
This module takes two parameter & return the mod function on elliptic curve.
mod (long int**,** ,long int, long int):
This module performs the inverse modular funtion. Like 5^{-1} mod(47).
char_num (char) - it return corresponding integer value for a string message.
Step4: num_char (int)
It returns corresponding conversion of integer value to string value.
Step5: Nop_Ordd(long int*,long int*, long int*,long int*, long int*,long int*):
This module performs the calculation of total number of point on elliptic curve. Also find its order. According to hess's law & Schoof algorithm.
Step6: sc_mul(long int*,long int* **,** long int* **,**long int* long int ,long int, long int):
This module perform scalar multiplication of elliptic curve point and a scalar by multiply add method.
Step7 Enter elliptic curve $y^2 = x^3+ax+b \bmod (p)$
Step8: Enter the value for parameter a, b, p such that $4*a^3+27*b^2! =0$"<<"\n";
Output will be:

Please enter your Private Key 3
Welcome in key generation
Key pair (148, 91)

Generation of Digital Signature:
Enter your message: e
Your digital signature (5, 9)
Verification:
W= 20
U1= 9
U2= 9
(Xv, Yv) = (148,151)
V0= 5, R=5 i.e. (V==r) so,
Digital Signature is verified.

7. Results and Discussion

In this paper, we will decide which approach is better for us in dealing with acoustic variability.

Elliptic curve cryptography (ECC):-

The most popular current alternatives are the elliptic curve cryptosystems (ECC) invented by Neal Koblitz and Victor Miller in 1985 independently. The security of elliptic curve cryptography depends on our inability to solve the elliptic curve discrete logarithm problem (ECDLP) in sub exponential time.
Many constraints for cryptography techniques like- RSA are –

- Band width Constraint.
- Memory Constraint.
- Execution Time Constraint

The following points summarizes the key benefits of elliptical curve cryptography

- **Less EEPROM and Shorter transmission.**
- **Scalability.**
- **No – Co-Processor.**

Applications of ECC:

ECC is particularly beneficial for application where:

- Computational power is limited (ICCs, wireless devices, PC cards).
- Integrated circuit space is limited (ICCs, wireless devices, PC cards).
- High speed is required.
- Intensive use of signing, verifying or authenticating is required.
- Signed messages are required to be stored or transmitted (especially for short messages).
- Bandwidth is limited (wireless communications and some computer networks).

Operation	Time (s)	Data mem (bytes)
ECC-160 point mult	1.6	282
RSA-1024 private key op	22	930

Elliptic Curve Cryptography provides greater security and more efficient performance than the first generation public key techniques (RSA and Diffie-Hellman) now in use. As vendors look to upgrade their systems they should seriously consider the elliptic curve alternative for the computational and bandwidth advantages they offer at comparable security.

Execution times and memory requirements favor ECC

8. Conclusion

Digital signatures provide cryptographic services that have become a necessity in data and network security. They offer non-repudiation, confidentiality, authentication, and integrity in a format that easily extends to the digital age. As systems become faster and smaller, they will need to maintain their security while using minimal resources. The elliptic curve digital signature algorithm provides the same functionality and security as the standard digital signature algorithm, but delivers it in a smaller key size. This makes it ideal for resource-constrained systems and network technology.
Elliptic curves offer major advantages over traditional systems such as increased speed, less memory and smaller key size. Although doing the group operations is slower for an ECC system than for RSA or other discrete log system of the same size, equal security can be provided by much smaller key length using ECC, to this extent that it can be faster than other Verify In addition, less storage, less power and less memory than other systems make it possible to implement cryptography in many special platforms such as wireless devices, laptop Computers and smart cards. So do the situations where efficiency is important.

9. Future Work

The application demonstrates the use of a moderately complex hybrid algorithm for data encryption –ECC. The future development of the application may use a more complex hybrid cipher techniques. This paper has already implemented the arithmetic operation like addition, subtraction, division efficiently but still some research can be done to make them better, although the project has been implemented as a stand-alone system it can also be implemented on the network environment.

The symmetric based ECC cryptosystem is somewhat slow, so some more research is needed to make it fast.

References

[1] George S. Oreku1, Jianzhong Li 1, 2, 1"Rethinking E-commerce Security "Department of Computer Science and Engineering Harbin Institute of Technology, Harbin 150001, China2Department of Computer Science and Engineering Heilongjiang University, Harbin 150080, China gsoreku@yahoo.com, lijzh@hit.edu.cn

[2] C.Barnes, Etal "Hack Proofing Your Wireless Networks", syngress Publishing, Rockland, MA, 2002.

[3] H. CHAN, ETAL "E-Commerce", Chichester, Wiley, 2 001.

[4] T. COLTMAN, ETAL "Keeping E-Business in Perspective", Communications of the ACM, August 2002 Vol. 45, no. 8, p. 69-73.

[5] A.K. GHOSH, "E-Commerce Security", New York, Wiley, 1998.

[6] S. KESH, S. RAMANUJAN, AND S. NERUR, "A Framework for Analysing E- Commerce Security" Information Management and Computer Security, 2002 Vol.10, no. 4, p 149-158.

[7] P.RATNASINGHAM "Trust in Web-Based Electronic Commerce Security", Information Management and Computer Security, 1998 Vol. 6, no. 4, p 162-166.

[8] Apache based Web DAV Server with LDAP and SSL htttp://www.unmelted.com

[9] William M. Daley, Secretary NATIONAL INSTITUTE O STANDARDS AND TECHNOLOGY, Raymond G. Kammer, Director.

[10] M.Tolga SAKALLI, Ercan BULU and Fatma BUYUKSARACOGLU Cryptography Education for Students Computer Engineering Department, Trakya University, Edirne { tolga. ercanb. fbuyuksaracoglu) @trakya.edu.tr.

[11] FIPS. 46-3, '"Data Encryption Standard," Federal Information Processing Standard (FIPS), Publication 46-3, National Bureau of Standards, US. Department of Commerce, Washington D.C... October 25. 1999.

[12] C. Smith, "Cryptography in the Algebra Class," NCT M Western Regional C conference, Phoenix. AZ. December 3.1999, "http://teachnet.edb.utexas.edu/-jenn/smit/nct/index. Html/ntro".

[13] Wiley & Sons, Inc. New York, 1996.A. Menezes, P.van Oorschot, S. Vanstone, Handbook of [13] ElGamal-Type Signature Schemes in Modular Arithmetic and Galois Fields

[14] Gerard J. Nealon Masters Project, Department of Computer Science Rochester Institute of Technology Rochester, NY USAgjn3855@cs.rit.edu July 15, 2005.

[15] David Bisjop Narsoa "Introduction to Cryptography htttp://www.Narsoa.com

[16] RSA Laboratoires. *PKCS #1 v2.1: RSA Encryptions Standard.* June 2002, <ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf

[17] Engelfriet, Arnoud. Elliptic Curve Cryptography. 1 Jan. 2004. 4 Apr. 2004. Ius Mentis.http://www.iusmentis.com/technology/encryption/elliptic-curves/>

[18] Hand Book of Cryptography Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone CRC Press The Elliptic Curve Digital Signature Algorithm (ECDSA). Canada: Certicom. 2001. Available at http://www.comms.scitech.susx.ac.uk/fft/crypto/ecdsa.pdf