ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

Study and Implementation of Elliptic Curve Encryption Algorithm for Azerbaijan E-ID Card

Mailov Arif [1], Abbasov Habib [2], Isayev Rufat [3], Safarov Azer [4]

Head of Certificate Services Centre, PhD, Data Processing Center, Ministry of Communications and High Technologies, Baku, Azerbaijan Republic[1]

Master of Computer Science, Data Processing Center, Ministry of Communications and High Technologies, Baku, Azerbaijan Republic[2]

Master of Applied Mathematics, Data Processing Center, Ministry of Communications and High Technologies, Baku, Azerbaijan Republic[3]

Bachelor of Applied Mathematics, Data Processing Center, Ministry of Communications and High Technologies, Baku, Azerbaijan Republic[4]

ABSTRACT: The aim of this paper is to examine performance of elliptic curve algorithms in comparison with Rivest, Shamir and Adelman (RSA) and clarify whether the elliptic curve cryptography is better suited for e-ID cards than RSA. We study performance and security of different elliptic curves and encryption algorithm using open source toolkit implemented in framework of the Java Cryptography Architecture. It is observed that the performance and security level of algorithms based on elliptic curves is significantly better than RSA based approach. The elliptic curve approach with smaller key sizes will provide a higher security and the faster execution time even without using a crypto processor in e-ID card chip.

KEYWORDS: e-ID card; elliptic curve; prime number; cryptosystem; security; crypto resistance; RSA; key length; ECDLP.

I. Introduction

The role of electronic identity cards (e-ID) is essential in harmonization of digital markets between different countries. In order to enable secure authentication and digital signature capabilities of e-ID card a Public Key Infrastructure should be established. This will provide high security for multiple applications in virtual environment and reliable access to e-government services.

Azerbaijan is planning to launch his national electronic identity cards (e-ID) in early 2007. This project should allow citizens to widely use such e-services as online banking, declaration of taxes and signing of contracts. The e-ID chip will contain two certificates and associated keys for authentication and digital signatures. The security of electronic services is accepted to be ensured by legally binding digital certificates of the National Certificate Services Centre. In order to meet smart card security and performance requirements the investigation of Elliptic Curve and RSA cryptosystems should be done. It is well known that main benefits of using Elliptic Curve cryptography in comparison with traditional RSA based cryptosystems are related with smaller key size for higher security, possibility to implement algorithm without crypto processor and faster execution time. There are only a few e-ID card providers which use elliptic curve cryptography [1] [2] [3].

DOI: 10.15680/ijircce.2015.0305150

This paper is organized as follows. Section II describes the related work carried out in research field decribed in the paper. In the Section III, the basic overview of Elliptic Curve Cryptography (ECC) is discussed. In Section IV the measurement results for different algorithms are compared. Finally, Section V presents the conclusions.

II. Related work

Cryptosystems with RSA and ECC algorithms are analysed over the years by many authors. Traditional RSA algorithm based on modular arithmetic with long operands was proposed by authors in [4]. The performance of RSA algorithm on processors with low memory and power is slow and computation time increases drastically as key size increase. In comparison with RSA algorithm Elliptic Curve Cryptography provides higher security with less key sizes and requires significantly less computational resources which make it attractive for use in digital signature smart cards. Comparative performance of several cryptographic algorithms is studied thoroughly by implementing them in Java language [5]. Performance evaluation of cryptosystems made by authors in detail is based on time measurements for key generation, encryption and decryption algorithms. The results of study are showed many advantages of ECC over the RSA.

III. Overview of Elliptic Curve Cryptography

Elliptic curve cryptography was suggested by Victor Miller [6] and Neal Koblitz [7] as alternative to traditional cryptography. This invention has solved the main problem of public key cryptography related with substantial increase of key length to meet a high level security requirement of cryptosystem.
A standard form of an elliptic curve E over the prime number field Z_p (where p is large prime number) is described by Weierstrass eq. (1)

$$\text{E:}\quad y^2 = x^3 + ax + b \ (\text{mod p}) \qquad \text{eq. (1)}$$

Two positive integers a, b ∈ Z_p, less than p are satisfy to non-singularity condition eq. (2).

$$4\,a^3 + 27\,b^2 \ (\text{mod p}) \neq 0 \qquad \text{eq. (2)}$$

For addition of two elliptic curve points P_1 (x_1, y_1) and P_2 (x_2, y_2) to produce a third point P_3 (x_3, y_3) on elliptic curve eq. (3) should be used

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \ \text{mod p} \\ y_3 &= \lambda\,(x_1 - x_3) - y_1 \ \text{mod p} \end{aligned} \qquad \text{eq. (3)}$$

, where

$$\lambda = \begin{cases} \dfrac{(y_2 - y_1)}{(x_2 - x_1)}, & \text{at } \ P_1 \neq P_2 \\ \dfrac{(3x_1^2 + a)}{(2y_1)}, & \text{at } \ P_1 = P_2 \end{cases}$$

In case of point multiplication any point P on elliptic curve multiplied with a scalar n gives another point Q on the same curve determined by eq. (4)

$$\text{Q} = \text{mP} \qquad \text{eq. (4)}$$

Formally, eq. (4) represents the point P added to itself m times. It is easy to determine a new point Q given values n and P, but it is very difficult to calculate n for known values P and Q. This problem is called the Elliptic Curve Discrete Logarithm Problem (ECDLP). Therefore computational solving of this problem is the basis of

For any specific elliptic curve the set of domain parameters a, b, p, n, G is defined as

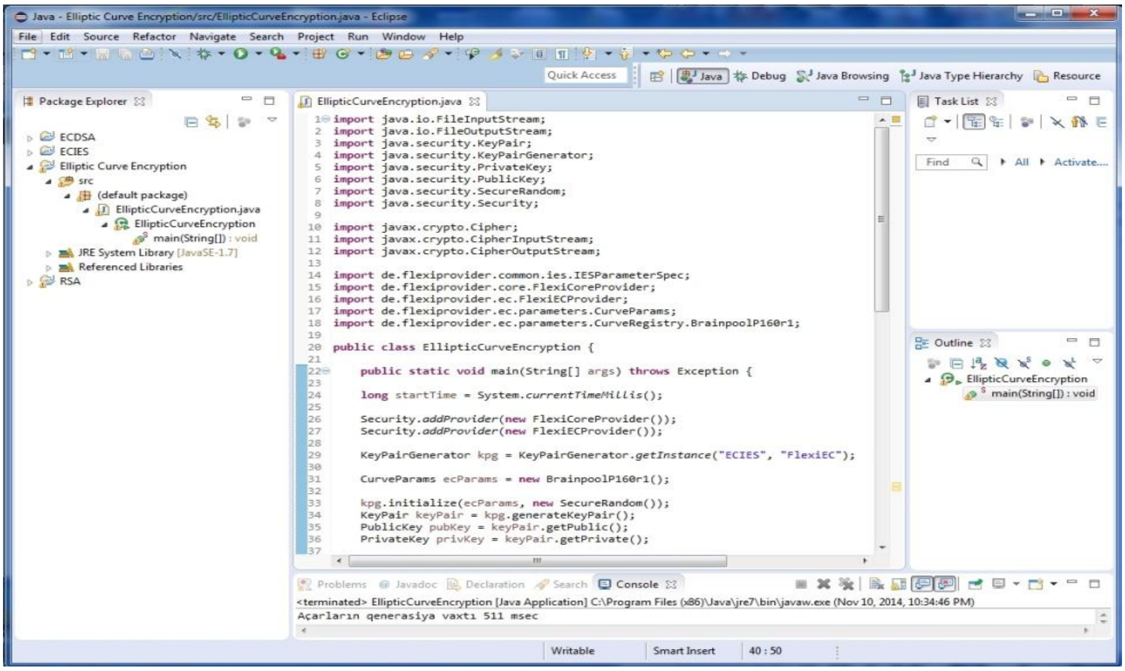
- a and $b \in Z_p$,
- $G = (x_G, y_G)$ is the generator of a cyclic subgroup of curve,
- n is the prime number indicating the order of G,
- p is the large prime number,

In cryptography the creation of cryptosystem requires determination of three algorithms: key generation, encryption and decryption. All parties agree on above mentioned domain parameters of elliptic curve and must know them. In elliptic curve cryptography key pair is associated with domain parameters and the public key is selected as a point on the curve while a private key is a random number chosen in the range [1, n-1]. The public key is determined by multiplying a point generator G of the order n on a private key.

Determination of algorithms for construction of cryptosystem and comparison the results obtained for different elliptic curves is discussed in the next subsections.

IV. THE IMPLEMENTATION AND ANALYSIS

The implementation environment for the chosen algorithms is Java JDK 8 update 45 and the platform for our measurements is Windows 7 Professional 64-bit, running on Intel(R) Core i7-2630QM CPU@ 2.00 GHz and 6.00 GB of RAM. Open source implementation of the interface is based on the framework of the Java Cryptography Architecture (JCA) / Java Cryptography Extensions (JCE) and underlying algorithms are integrated with the Flexi Provider [8] toolkit developed at the Theoretical Computer Science - Cryptography and Computer Algebra Department of TU Darmstadt.



```
import java.io.FileInputStream;
import java.io.FileOutputStream;
import java.security.KeyPair;
import java.security.KeyPairGenerator;
import java.security.PrivateKey;
import java.security.PublicKey;
import java.security.SecureRandom;
import java.security.Security;

import javax.crypto.Cipher;
import javax.crypto.CipherInputStream;
import javax.crypto.CipherOutputStream;

import de.flexiprovider.common.ies.IESParameterSpec;
import de.flexiprovider.core.FlexiCoreProvider;
import de.flexiprovider.ec.FlexiECProvider;
import de.flexiprovider.ec.parameters.CurveParams;
import de.flexiprovider.ec.parameters.CurveRegistry.BrainpoolP160r1;

public class EllipticCurveEncryption {

    public static void main(String[] args) throws Exception {

    long startTime = System.currentTimeMillis();

    Security.addProvider(new FlexiCoreProvider());
    Security.addProvider(new FlexiECProvider());

    KeyPairGenerator kpg = KeyPairGenerator.getInstance("ECIES", "FlexiEC");

    CurveParams ecParams = new BrainpoolP160r1();

    kpg.initialize(ecParams, new SecureRandom());
    KeyPair keyPair = kpg.generateKeyPair();
    PublicKey pubKey = keyPair.getPublic();
    PrivateKey privKey = keyPair.getPrivate();
```

```
<terminated> EllipticCurveEncryption [Java Application] C:\Program Files (x86)\Java\jre7\bin\javaw.exe (Nov 10, 2014, 10:34:46 PM)
Açarların qenerasiya vaxtı 511 msec
```

Fig.1. Program code for encryption and decryption of plaintext Elliptic Curve Cryptography algorithm.

Due to security reasons not all elliptic curves are suitable for use. Only those curves with well understandable properties shall be selected for investigation. In our implementation the following recommended NIST [9], Certicom [10] and Brainpool curves [11] are used:

- BrainpoolP160r1 - BrainpoolP512r1,
- Secp112r1 - Secp521r1,

- Secp160k1 - Secp256k1.

The program code shown in Fig.1generates a key pair (valid public key for encryption and private key for decryption) using BrainpoolP160r1curve and performs encryption and decryption of fixed size plaintext. Encryption and decryption scheme based on ECC is the Elliptic Curve Integrated Encryption Scheme (ECIES) described elsewhere [12].

We are compared the performance of elliptic curve encryption algorithms with RSA in terms of key generation time as a function of key sizes. The results of measurements of encryption and decryption time for different elliptic curves in comparison with the RSA are presented in Table I. As expected, the key pair generation time as well as encryption and decryption time increases about linearly with the key size, while the difference in a few orders of magnitude is observed between key pair generation time for elliptic curve and RSA algorithms.

TABLE I. Key pair generation, encryption and decryption time as a function of key sizes for different elliptic curves.

Type of elliptical curve	**Key length (bit)**	**Key generation time (msec)**	**Encryption time (100Kb plaintext) (msec)**	**Decryption time (100Kb plaintext) (msec)**
BrainpoolP160r1	160	5	22	32
BrainpoolP192r1	192	7	28	39
BrainpoolP224r1	224	9	38	49
BrainpoolP256r1	256	12	47	62
BrainpoolP320r1	320	19	72	94
BrainpoolP384r1	384	31	103	140
BrainpoolP512r1	512	66	201	299
NIST curves				
Secp112r1	112	3	16	26
Secp160r1	160	5	23	32
Secp224r1	224	8	32	53
Secp256r1	256	12	41	68
Secp320r1	320	17	53	83
Secp384r1	384	28	102	125
Secp512r1	512	68	227	279
Certicom curves				
Secp160k1	160	4	19	32
Secp192k1	192	6	24	38
Secp224k1	224	8	30	47
Secp256k1	256	11	37	56
RSA				
RSA512	512	46	52	53
RSA1024	1024	307	312	293
RSA2048	2048	2777	2896	3011
RSA3072	3072	12898	23668	14157
RSA4096	4096	42619	49196	38892

It becomes clear that elliptic curve algorithms will significantly reduce the cost of e-ID card production due to fast key generation and small memory requirements.
In Fig.2 shown comparison of time required for solving of ECDLP problem with the time required for solving Integer Factorization Problem. Complexity of the solution ECDLP problem depending on the number of bits n in the input is expressed by eq. (5).

$$C_{ECDLP\,(n)} \approx 2^{n/2} \qquad \text{eq. (5)}$$

It is seen from Fig.2. ECC 256-bit provides the same level of security to RSA 3072 and ECC 384-bit provides comparable security to RSA 7680-bit.

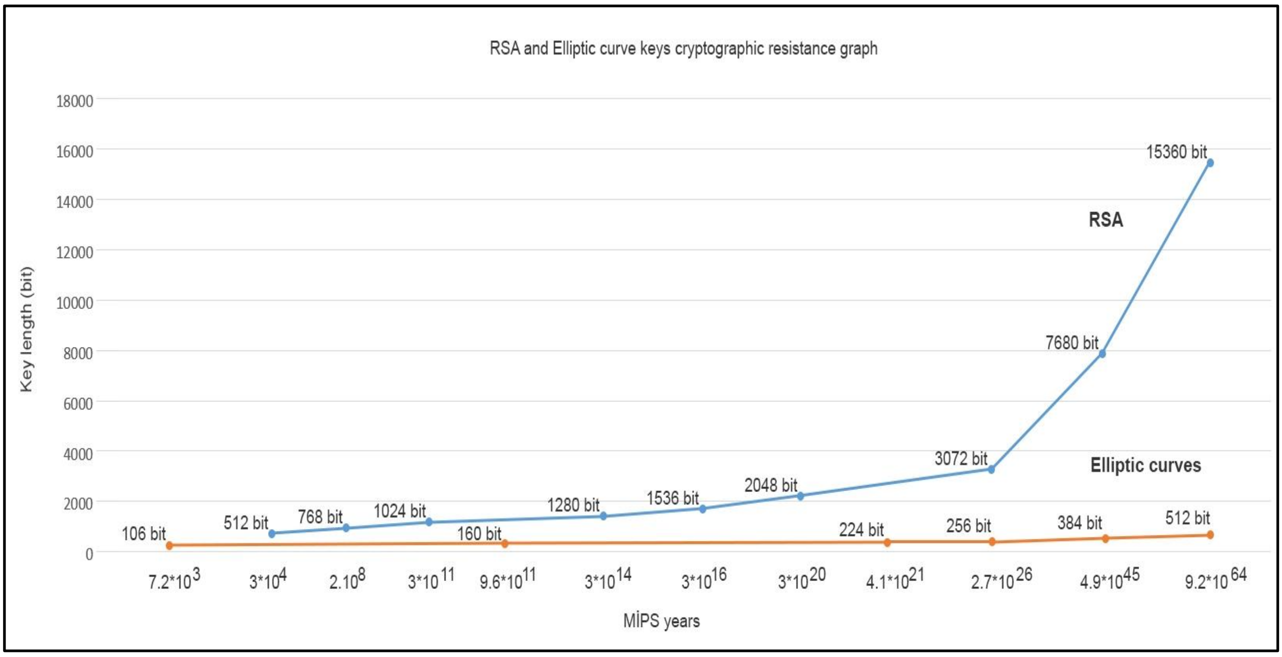


Fig.2. Comparison of crypto resistance of algorithms based on elliptic curve and RSA

The running time is computed in MIPS-year which is equal to the number of steps processed by computer for one year at one million instructions per second.

V. Conclusion

The measurements showed that using elliptic curve algorithms in e-ID card production will provide high efficient performance and greater security in comparison with traditional RSA algorithm. When large volumes of e-ID cards are expected to be produced, elliptic curves are better than RSA.

VI. Acknowledgment

The authors would like to thank Dr. Nail Mardanov, Director of Data Processing Center, for his encouragement and inspiration to work on this current research topic. This work was supported by the Science Development Foundation under the President of the Republic of Azerbaijan - **Grant № EIF-RITN-MQM-2/IKT-2-2013-7(13)-29/19/1**.

REFERENCES

1. Tauber, A., Zefferer, T., and Zwattendorfer, B., "Approaching the Challenge of e-ID Interoperability: An Austrian Perspective", European Journal of ePractice, Number 14, pp. 22-39, 2012.
2. Leitold, H., Hollosi, A., Posch, R., "Security Architecture of the Austrian Citizen Card Concept", Proceedings 18th Annual Computer Security Applications Conference, pp.391-400, 2002.
3. BSI, "Elliptic Curve cryptography", TR-03111, version 2.0, 2012.
4. Rivest, R.L., Shamir, A., and Adleman, L., "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, Vol. 21, No.2, pp. 120-126, 1978.
5. Alese, B.K., Philemon, E.D., and Falaki S.O., "Comparative Analysis of Public-key Encryption Schemes", International Journal of Engineering and Technology, Vol.2, No 9, pp. 1552 - 1568, 2012.
6. Miller, V.," Use of elliptic curves in cryptography", Proceedings CRYPTO'85, Springer-Verlag, pp. 417-426, 1986.
7. Koblitz, N., "Elliptic curve cryptosystems", Mathematics of Computation, Vol. 48, Number 177, pp. 203- 209, 1987.
8. Buchmann, J., Coronado Garcia, L.,C., Dahmen, E., Döring, M., and Klinsevich, E., "CMSS - An Improved Merkle Signature Scheme", Proceedings 7th International Conference on Cryptology in India, Vol. 4329, pp. 349-363, 2006; The FlexiProvider group at Technische Universitat Darmstadt. Flexiprovider, "A Provider for the Java Cryptography Architecture", http://www.flexiprovider.de, 2015.
9. National Institute of Standards and Technology (NIST) , "Recommended Elliptic Curves for Federal Government Use", http://csrc.nist.gov/groups/ST/toolkit/documents/dss/NISTReCur.pdf, July, 1999.
10. Certicom, "Standards for Efficient Cryptography, SEC 2: Recommended Elliptic Curve Domain Parameters", version 2.0, 2010.
11. Lochter, M., and Merkle, J., "ECC Brainpool Standard curves and Curve Generation", RFC 5639, pp. 1-27, 2010.
12. Abdalla, M., Bellare, M., and Rogaway, P., "The Oracle Diffie-Hellman Assumptions and an Analysis of DHIES", Topics in Cryptology - CT-RSA 2001, Vol. 2020, pp. 143-158, 2001.

BIOGRAPHY

Mailov Arif is a Head of National Certificate Services Centre, Ministry of Communication and High Technologies of Azerbaijan Republic. He received PhD in Mathematics in 1996 from JINR, Dubna, Russia. His research interests are Cryptography, C programming etc.

Abbasov Habib is a Deputy Head of National Certificate Services Centre. He received Master of Computer Sciences degree in 2014 Azerbaijan State University, Baku, Azerbaijan. His research interests are electronic signature, cryptography and Public Key Infrastructure etc.

Safarov Azer is a Program Developer in Data Computing Centre, Ministry of Communication and High Technologies of Azerbaijan Republic. He received Master degree in Mathematical Statistics in 2015 from Baku State University, Baku, Azerbaijan. His research interests are web, Java and mobile programming etc.

Isayev Rufat is a Program Developer in the Data Computing Centre, Ministry of Communications and High Technologies. He received Bachelor degree in Computer Engineering in 2014 from Azerbaijan State Oil Academy, Baku, Azerbaijan. His research interests are web programming, C# etc.