UDK 517.538 (083.73) (045)

ELLIPTIC CURVE CRYPTOGRAPHY

O. O. Meleshko*, *O. O. Kovalskiy

Національний авіаційний університет

porcupine-koval7@yandex.ru

Розглянуто структуру еліптичної криптографії, її вигляд,основне застосування. Схарактеризовано основні переваги використання еліптичної криптографії з-поміж РСА та іншими. Викладено основні історичні дати про цю гілку криптографії. Зібрано основні дані про патенти, що її стосуються — запропонованих NIST. Надано порівняння РСА та еліптичної криптографії у вигляді таблиці. Вважалось,що еліптичні криві матимуть успіх у криптографії через деякі їх властивості, такі як довжина ключа, менша вибагливість до продуктивності, надійності. Еліптичні криві використовуються для передачі даних по TLS, SSH, смарт-картах, Bitcoin,C++, Apple's і Message service. Зараз питанням еліптичних кривих активно займаються керуючий комітет «ECC Workshops» на чолі з Tanja Lange (Technische Universiteit Eindhoven, Netherlands), Chair Alfred Menezes (University of Waterloo, Canada , Christof Paar (Ruhr — Universität Bochum, Germany), Scott Vanstone (University of Waterloo, Canada).

ECC Workshop — це щорічні семінари, присвячені вивченню еліптичної криптографії та суміжних їй областей. С першого семінару в 1997 р. в Ватерлоо конференція з еліптичних кривих розширила свою сферу діяльності за межі еліптичної криптографії і наразі охоплює широкий спектр в областях сучасної криптографії.

Ключові слова: еліптична криптографія, криптографія з відкритим ключем, помноження, зашифрувати, підпис, гіпереліптична крива, аутентифікація.

In this article the structure of elliptic cryptography,its shape and main points of application is reviewed.We examined advantages of using ECC comparing with RSA and others. Main dates about this branch of cryptography is described. We put together information about patents, relating to this theme. Also in this article the question about if we should trust to NIST recommended curves is bumbed. As the conclusion we give comparing table ECC and RSA.

Thoughts that Elliptic curves will be successful as to their key length, less demanding performance, security. Elliptic Curves are used to pass data through TLS, SSH,also used in smart-cards,Bitcoin, C++, Apple's i Message service.

Now the steering committee is actively engaged on ECC in the head of Tanja Lange (Technische Universiteit Eindhoven, Netherlands), Chair Alfred Menezes (University of Waterloo, Canada), Christof Paar (Ruhr-Universität Bochum, Germany), Scott Vanstone (University of Waterloo, Canada).

ECC is an annual workshops dedicated to the study of elliptic curve cryptography and related areas. Since the first ECC workshop, held 1997 in Waterloo, the ECC conference series has broadened its scope beyond elliptic curve cryptography and now covers a wide range of areas within modern cryptography.

Keywords: elliptic curve, Public key cryptography, multiplication, encipher, signature, hyperelliptic curve, authentication.

Introduction

Elliptic curve cryptography (ECC) is one of the most powerful branch of cryptography. ECC secure everything from HTTPS (Hyper Text Transfer Protocol Secure) connections to data transfer between data centers. An elliptic curve is a set of point-the smooth curve on the Cartesian plane, described by the following equation

$$y_2 + a_1xy + a_3y = x_3 + a_2x_2 + a_4x + a_6,$$

that was called as originally elliptic curve.

If all unknown variables — real numbers, by replacement of variables the equation can be transformed to

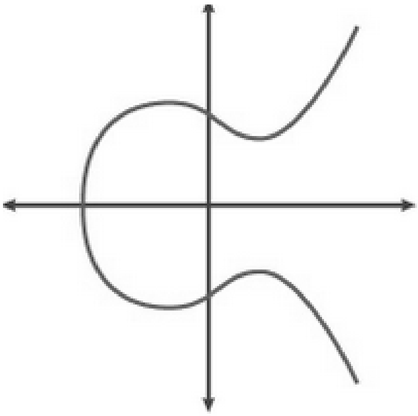
$$y^2 = x^3 + ax + b.$$

Basic view of elliptic curve is given on the picture 1.

ECC is considered to be much more secure and usefull than RSA and other first-generation public key cryptography systems.

Public key cryptography means that we use two separate keys, public and secret key. The public key is used to encrypt plaintext and the private key is used to decrypt cipher text.

In general public key algorithms are based on mathematical problems which admit no efficient solution, as integer factorization, discrete logarithm.



Picture 1

The security of the RSA cryptosystem is based on two mathematical problems: the problem of factoring large numbers and the RSA Problem. The RSA algorithm raises a message to an exponent, modulo a composite number N whose factors are not known. RSA problem consists in finding the eth roots of an arbitrary number, modulo N. Full decryption of an RSA cipher text is thought to be impracticable on the guess that both of these problems are hard, so there are no efficient algorithm to solve them.

After the introduction of RSA researchers were looking for other algorithms that would serve as good trapdoor functions.Then cryptographic algorithms were proposed based on branch of mathematics called elliptic curves. Main advantages and disadvantages comparing ECC and RSA are given in Table.

Comparing RSA and Elliptic Curve Cryptography	
RSA	Elliptic Curve Cryptography
The RSA algorithm is the most popular and best understood public key cryptography system, RSA is older then ECC and is already wide used	Much more younger than RSA, not at least explored
	On many platforms, ECDSA operations computed faster than similar strength RSA or DSA
RSA is based on problem of factoring large numbers and the RSA Problem	ECC is assumed that finding the discrete logarithm of a random elliptic curve element to a base point is infeasible, it is as known ECDLP
Symmetric Key Size(bits)	RSA and Diffie-Hellman Key Size(bits)

End table

Comparing RSA and Elliptic Curve Cryptography

Symmetric Key Size(bits)	RSA and Diffie-Hellman Key Size(bits)	Elliptic Curve Key Size(bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Ratio of DH computation versus EC computation for

Security level(bits)	Ratio of DH costs : EC Cost
80	3:1
112	6:1
128	10:1
192	32:1
256	64:1

each of the key sizes

ECC's security consists in multiplying a point on the curve, but it will produce another point on the curve, so it is very difficult to find what number was used, even if you know the original point and the result. There are two ways to multiply a point: recursion or use of addition and doubling with the binary method for multiplication .Equations based on elliptic curves have a characteristic that is very beneficial for cryptography: they are easy to perform, and difficult to reverse.

The idea to use elliptic curves in cryptography was proposed by Neal Koblitz and Victor S. Miller in 1985. N. Koblitz proposed to consider on symbols of arbitrary alphabet A, where each letter corresponds to its number m. Number m encodes by point $P(x, y)$.In this way we translate our alphabet into a set of point on an elliptic curve.

In 2006 this algorithm was accepted by National Institute of Standards and Technology. H. W. lenstra, a dutch mathematican proposed a new integer factorization algorithm, based on arithmetic of elliptic curves, which use a negligible amount of storage.

We should pay attention on following details, if we are going to use elliptic cryptography: algorithm for multiplication on an elliptic curve, and to choose a right point on the curve. It is no less important what information needs to be transmitted.

For the schemes based on complexity of a problem of logarithming in discrete fields, transition to elliptic curves allows to increase firmness significantly. It is caused by a choice of parameters of a curve the problem of logarithming in group of points of a curve is significantly more difficult than a problem of logarithming in multiplicative group of an initial field.

ECC's problem

The main problem is popularity of ECC, as we know ECC is much more younger than RSA, but it is also in demand: the US government uses it to protect internal communications, as called Tor project — the mechanism to prove ownership of bitcoins, it provides signatures in Apple's i Message service. ECC is used to encrypt DNS (Domain Name System) information with DNS Curve, and for authentication for secure Web browsing. A growing number of sites use ECC to provide online privacy. Motorola has incorporated Certicom's ECC in its handsets and RIM in its Blackberry hand computers.

The Aim

The aim of this article is to systematize information on the practical application of elliptic curves,its general terms, compare RSA and ECC, affect the topic of ECC popularity.

Implementation of ECC

Surely, ECC is in wide use in programing, for example in C++ a library "Libecc" intended for enciphering on an elliptic curve which supports keys of the fixed size for achievement the maximum speed of work. Also ECC is used in NaCl Library, it include Curve25519.

Bitcoin, SSH (Secure Shell), TLS (Transport Layer Security) and Austrian e-ID cards is another example of protocols, that also enjoy ECC.

Bitcoin is an electronic crypto-currency, elliptic curve cryptography is central to its operation. Public keys and signatures are publicly available and auditable, it helps to prevent double-spending.

Bitcoins transaction uses digital signatures, but their addresses gain from elliptic-curve public keys.

Bitcoin block chain consists all transactions ever executed. Each block of this journal consists the SHA-256 hash of the previous block.

The signatures, used in Bit coin are ECDSA (Elliptic Curve Digital Signature Algorithm), where the curve secp256k1 is used. There are over 11 million bit coins in value of over 2 billion USD in circulation.

As to SSH, elliptic curve cryptography can be used in three positions.

Clients can use ECDSA public keys for client authentication. The ephemeral Elliptic Curve Daffier Hellman key exchange method is used in SSH: each server has a host key to authenticate itself to the client, server authenticate itself by sending a transcript of the key exchange

Elliptic curves also takes place in TLS protocol. RFC 4492 specifies elliptic curve cipher for TLS.ECC was added to TLS through an additional set of cipher suites, cipher suites help with identity verifiaetion, selection of key exchange, encryption, message authentication.

TLS server does not send its full preference of cipher suites, instead of this the client sends its list of supported elliptic curves and cipher suites and server choose suitable one from this list.

ECC is effective in smart cards and Cryptographic tokens, Smart cards have extremely rigid constraints on processing power, parameter storage, and code space. Smart cards are deployed for user authentication, they contain cryptographic hardware modules.

Austria's e-ID cards may contain ECDSA or RSA public key.

Certicom's researches and patents

Certicom has done extensive research on card implementations. The use of ECC is strongly recommended with NAND flash parts owing to their tendency to occasionally bit-flip. The NAND library comes with a software ECC implementation named linux_mtd_ecc. Sony use ECC in Advanced Access Content System and Digital Transmition Content Protocol.

ECC algorithm was patented by the Certicom company's founders. It is one of the main factors limiting its wide acceptance, the Open SSL team accepted an ECC patch only in 2005, despite that it was submitted in 2002 .Though some alternative techniques of ECC are not covered by the patents.

There are such wide-known patents, as patent on technique of validating the key exchange messages using ECC to prevent a man-in-the middle attack ,patent on techniques for compressing elliptic curve point representations, patent on calculating the x-coordinate of the double of a point in binary curves via a Montgomery ladder in projective coordinates, a patent on efficient GF(2n) multiplication in normal basis representation, they all belongs to Certicom. Exception is Hewlett-Packard's U.S. Patent 6,252,960 on compression and decompression of data points on elliptic curves. So, Certicom holds over 130 patents relating to elliptic curves and public key cryptography in general. In 1998 Certicom developed Standards for Efficient Cryptography Group to develop commercial standarts for cryptography based on elliptic curve cryptography.

ECDS was accepted in 1999 as ANSI standart, and became IEEE (Institute of Electrical and Electronics Engineers) and NIST (The National Institute of Standards and Technology) standart in

2000. Digital Signature schemes can be used to provide data origin authentication and non-repudiation, data integrity. ECDSA was first proposed in 1992 by Scott Vanstone.

Elliptic Curve Digital Signature Algorithm is used in XML Signatures. Algorithm is specified in [XMLDSIG]. [XMLDSIG] defines two digital signature methods: RSA and DSA (DSS) signatures. ECDSA signaturesis is used as an additional method.

ECDSA incorporates the use of a hash function. Currently, the only hash function defined for use with ECDSA is the SHA-1 message digest algorithm [FIPS-180-1].

ECDSA signatures are smaller than RSA, public keys and certificates are smaller than similar strength DSA keys.

On many platforms, ECDSA operations computed faster than similar strength RSA or DSA operations. These advantages make ECDSA an attractive choice for XMLDSIG implementations.

Can we trust to the NIST recommended curves?

Also it is important to make attention on the NIST recommended elliptic curves over prime field. The National Institute of Standards and Technology (NIST) has standardized on a list of 15 elliptic curves of varying sizes. Ten of these curves are for what are known as binary fields and 5 are for prime fields. Prime fields are so, that the bit length of their orders are at least twice the key length of common symmetric-key block ciphers. Fast reduction for the NIST primes was much faster then Barrett.

Daniel Berstein and Tanja Lange were working on understanding the reason why do people choose standardization curves, how the standarts get implemented, what is wrong with the NIST curves. The conclusion is that people use standardized curves as they trust to standards committee.

In the WEB there are a lot of topics about if we should use NIST-recommended curves, ECC parametrs. Frank Konkel wrote in FCW-“Top-secret documents leaked by former National Security Agency contractor Edward Snowden confirm that the NSA introduced weaknesses into computer security standards adopted by the National Institute of Standards and Technology, putting at risk NIST's reputation as a disinterested purveyor of cyber guidelines”[3].

If you implement the NIST curves, there is a great chance that you doing it in a wrong way, as a result your code produces an incorrect results for some rare curve points, your code leaks secret data and these problems are exploitable by attackers. Huge timing channel, NIST curves passes all tests but still has failure cases are another disadvantages of NIST curves.

As conalusion the author advices to use Montgomery curves with unique point of order 2, choose twist-secure curves.[2]

A study of ECC implementation in software for constrained devices such as smart cards, in hardware would be beneficial to practitioners. Comparsion of the implementation of ECC and RSA and discrete logarithm system on various platform, performance of signature schemes based on elliptic curves, implementation of elliptic curve cryptosystems over GF(p) on a 16-bit microcomputer may become an important step in studying ECC.

Inference

Since 1997 were hold a series of conferences on the ECC theme, called “Workshop on Elliptic Curve Cryptography”. Last event tacked place in Queretaro, Mexiko in October. Speakers discussed pairing-based cryptography, voting protocols ,side-channel attacks, quantum key distribution, AES, hash functions, hyper elliptic curve cryptography.

So, ECC provides much more confidence use than first-generation public key cryptography systems. Equations based on elliptic curves is easy to perform, and extremely difficult to reverse and it is in demand. With ECC, you can use smaller keys to get the same levels of security. Small keys are important, especially in a world where more and more cryptography is done on less powerful devices like mobile phones. ECC appears to offer a better tradeoff: high security with short, fast keys. ECDSA is now an ANSI, IEEE, NIST standart.

LITERATURE

1. *Miller V.*, Uses of Elliptic Curves in Cryptography, Advances in Cryptology-Crypto’85, Lecture Notes in Computer Science. — Vol. 218, Springer, Berlin, 1986. — P. 417–426.

2. *Elaine Barker*, William Narker and others, NIST Special Publication 800-57 Part1, Computer Security Revised 2007, NIST. — 142 p.

3. *Joppe W.*, Bos J., Alex Halderman, Nadia Heninger, Jonathan Moore, Michael Naehrig, Erik Wustrow “Elliptic Curve Cryptography in Practise“ Microsoft Research,University of Michigan. University of Pennsylvania. — 16 p.

4. *Neal Koblitz* “Introduction to Elliptic Curves and Modular Forms” Springer-Verlag. — New York–Berlin Heidelberg–Tokyo, 1984. — 320 p.

Стаття надійшла до редакції 06.05.2014.