УДК 681.3

**Ақшолақ Г.И., Мағазов Р.С.**
әл-Фараби атындағы Қазақ Ұлттық университеті
Алматы, Қазақстан
Ғылыми жетекші: Дуйсебекова К.С.

# ЭЛЛИПТИКАЛЫҚ ҚИСЫҚТАРДЫҢ АҚПАРАТТЫ ҚОРҒАУДА ҚОЛДАНЫЛУЫ

***Аңдатпа.*** *Мақалада эллиптикалық қисықтар, оның криптографияда қолданылуы және басқа ашық кілтті криптографиялық жүйелерден артықшылықтары туралы басты мәліметтер берілген. Эллиптикалық криптографияны аппараттық іске асыру платформасы ұсынылған.*

***Кілт сөздер:*** *эллиптикалық қисықтар, ECC, RSA, ашық кілтті криптожүйе, ASIC және FPGA платформалары*

## Кіріспе

1985 жылы Нил Коблиц пен Виктор Миллер ашық кілті бар криптожүйелерде эллиптикалық қисықтарды пайдалануды ұсынды [1,2]. Осы уақыттан бастап криптография саласында «Эллиптикалық қисықтардағы криптография (Elliptic Curve Cryptography – ECC)» термині пайда болып, дамудың жаңа бағыты басталды. Криптографияда эллиптикалық қисықтарды қолдану сымсыз байланыстың – жоғары жылдамдығы және кілттің шағын ұзындығына байланысты туындады.

ECC – ашық кілттер криптографиясы саласындағы деректерді неғұрлым қауіпсіз таратуда пайда болған ең заманауи технология. Бұл технология RSA және Диффи-Хеллман сияқты ашық кілттерді шифрлаудың көптеген әдістерімен бірге қолданыла алады.

ECC басқа асимметриялық криптожүйелерге қарағанда, негізгі артықшылығы, өндеуге және есептеуге жұмсалған бірдей шығындарда және оның жоғары крипто-беріктігінде болып табылады. Себебі, эллиптикалық қисықтарда кері функциялардың есептеуі, дискретті логарифмді есептеуге (Диффи-Хеллман және Эль-Гамаль алгоритм-дері) немесе факторизациялау есебін шешуге (RSA алгоритмі) қарағанда, өте күрделі болып табылады. Нәтижесінде, бірдей беріктік деңгейге жету үшін, мысалы RSA алгоритмінде 1024 битті модуль қажет болса, эллиптикалық қисықтарға негізделген жүйелерде модуль мөлшері 164 бит ғана болады.

Эллиптикалық қисық деп келесі теңдеуді қанағаттандыратын (x,y) көп нүктесін айтады [3,4]:

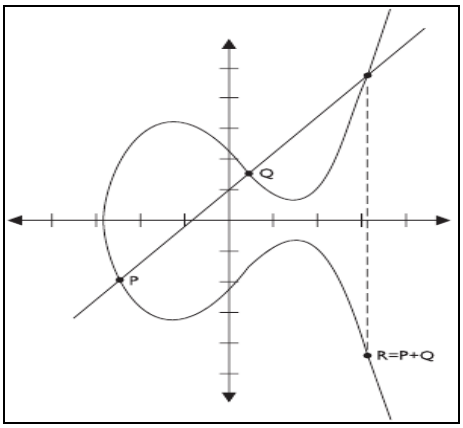
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Криптографияда келесі түрдегі қисықтарды қарастырамыз (Вейерштрасс формасы):

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

Бұл теңдеуді еркін өрістерге, әсіресе криптография үшін ерекше қызығушылық тудыратын шектеулі өрістерге қатысты қарастырамыз.

Эллиптикалық қисықтың типтік нұсқасының графигі 1-суретте көрсетілген. Эллиптикалық қисықтар үшін келесі теңдеу орындалады: $4a^3 + 27b^2 \neq 0$. Сингулярлы қисықтар үшін бұл шарт орындалмайды.




*Сурет 1 - Эллиптикалық қисықтың типтік графигі*

**Криптографияда эллиптикалық қисықтардың қолданылуы**

Криптографияда эллиптикалық қисықтардың екі түрі қарастырылады: $Z_P$ (қарапайым санның модулі бойынша шегерімдер сақинасы) және $GF(2^m)$ (бинарлы соңғы өріс). $GF(2^m)$ өрісінде эллиптикалық қисықтардың бір маңызды артықшылығы бар, $GF(2^m)$ өрісінің элементтері n - биттік кодтық сөздер түрінде оңай ұсынылуы мүмкін. Бұл эллиптикалық алгоритмдерді аппараттық іске асыру жылдамдығын арттыруға мүмкіндік береді [5]. Көп зерттеулерде екілік шектеулі $GF(2^m)$ өрісіне негізделген ECC енгізу тандалады, себебі бұл нақты математикалық құрылым ECC аппараттық және бағдарламалық жүзеге асырылуларында тиімді нәтижелер береді.

Эллиптикалық қисықтарда топтар туралы түсінік маңызды рөл атқарады. Эллиптикалық қисықтың нүктелерінің жиынтығында топ эллиптикалық қисық нүктелерінің қосылуымен анықталады. P және Q нүктелерінің қосындысы үшінші нүкте R деп аталады. Ол PQ түзуінде және элиптикалық қисықтарда жатады және R=P+Q , яғни –R+P+Q=0 болады. Оны 1-суреттен де байқай аламыз. Сонымен қатар эллиптикалық қисықтарды қосу кезінде нүктелер бір біріне жақын орналасуы мүмкін. Ол кезде жоғарыдағы қосу амалын қолданамыз. Кейбір жағдайда екі нүкте бір орында тұрады, яғни P=Q. Бұл кезде де қосу амалын орындауға болады. Алайда екі нүктені қосу нәтижесін біле отырып, қанша операция орындалғанын табу өте қиынырақ. Яғни nP=R, n=?. Бұл жерде x,y параметрлері нешеге тең деген тағы бір сұрақ туындайды.

x,y параметрлері шексіздікке тең болады: $x_{max} = \infty$, $y_{max} = \infty$.

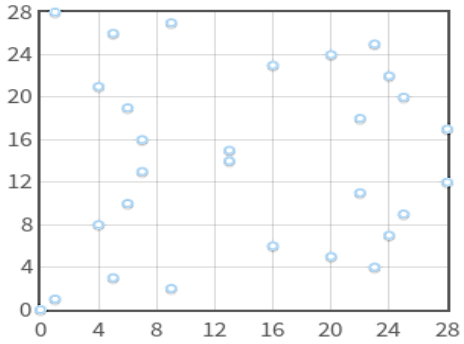
Ол кезде жоғарыда берілген теңдеу келесідей өзгереді және ол эллиптикалық криптографияда қолданылады, яғни дискретті логорифмге жүгінеміз. Криптографияда эллиптикалық қисық тек нүктелерден тұрады (2-сурет) [6].

$$y^2 = x^3 + ax + b \bmod p$$

$$4a^3 + 27b^2 \neq 0 \bmod p.$$

ECC дамуының бірінші бес жылдығынан кейін оны бағдарламалық жүзеге асырумен қатар аппараттық іске асыру кеңінен қарастырыла бастады. Мұның себебі ашық кілтті криптожүйелер сол уақыттағы дербес компьютерлердің жалпы мақсаттағы процессорларында баяу жұмыс жасады. Сондықтан қандай да бір аппараттық жеделдету қажет болды.

Аппараттық қамтамасыз етуге ECC енгізу жылдамдық және өлшем секілді бірнеше себептер бойынша қажет және тиімді болып саналады. ECC аппараттық іске асыру $GF(2^m)$ екілік өрісінде тез жүзеге асады.




*Сурет 2 - Криптографиядағы эллиптикалық қисық нүктелері*

Ашық кілтті алгоритмдер үшін аппараттық іске асыру кезіндегі негізгі мәселе мақсатты платформаны таңдау болып табылады. Таңдау кезінде келесі екі платформаның бірін алуға болады – олар ASIC және FPGA платформасы. Көптеген зерттеулерде FPGA платформасы таңдалады [7].

FPGA платформасы жылдам дизайн циклы және капиталды азайту секілді артықшылықтарымен сипатталады. FPGA платформасы өнеркәсіпте де ерекше танымал болып келеді.

Жоғарыда айтылған пайымдаулар мен жүргізген зерттеулер негізінде эллиптикалық криптографияның келесідей артықшылықтарын атаймыз:

1) Кілттің салыстырмалы қысқа ұзындығы;

2) Эллиптикалық алгоритмдердің жылдамдығы классикалыққа қарағанда, тез болып табылады. Бұл өріс өлшемімен және компьютерлер үшін жақын екілік өріс құрылымын қолданумен түсіндіріледі.

3) Кілттің кішкентай ұзындығына және жоғары жұмыс жылдамдығына байланысты ECC алгоритмдері смарт – карталарда және басқа да есептеуіш мүмкіндіктері шектеулі құрылғыларда пайдаланылады.

Асимметриялық криптографияда эллиптикалық қисықтарды қолдану ашық кілттерді құрудың негізгі және ең сенімді технологияларының бірі болып табылады. Мұндай криптографиялық жүйелердің тұрақтылығының негізгі өлшемі дискретті логарифмді шешудің күрделілік мәселелері болып есептеледі.

**Эллиптикалық криптографияның қолдану аясы**

ECC келесі заманауи жүйелерде қолданылады:

1) Ірі бизнес ұйымдарының ақпараттық жүйелерінде. Ірі бизнес кәсіпорындары өзінің коммерциялық құпиясын қорғау кезінде баға мәселелері екінші жоспарға кетеді. Мұнда CSP VPN бағдарламалық кешені сияқты сертификатталған ақпаратты қорғау құралдары қолданылады.

2) Орта және шағын бизнесті ұйымдастырудың ақпараттық жүйелерінде. Мысалы, ЭЦҚ rutoken идентификаторлары, eToken ГОСТ.

3) Мобильді саудада. Бұл ортада мәліметтерді таратудың әртүрлі хаттамалары қолданылады, мысалы, ұялі телефондарда, қалта планшеттерінде және т.б. WAP мәліметтерді таратудың сымсыз хаттамалары қолданылады.

4) Мемлекеттік мекемелердің ақпараттық жүйесінде. ЗАСТАВА, CPN VPN Server секілді әртүрлі сертификатталған кешендер қолданылады.

5) Банктік мекемелердегі операцияларды орындауда.

6) Интернет – қосымшаларда. Бұл жерде эллиптикалық қисықтар алгоритмдерімен криптографиялық хаттамаларды қолдану кеңінен тараған, мысалы, Secure Sockets Layer (SSL) – соккеттермен қорғалған криптографиялық хаттамалар [8,9].

**Қорытынды**

Көптеген зерттеулерді сараптай келе, эллиптикалық қисықтарды модуль бойынша қарапайым есептеулермен салыстырғанда, эллиптикалық қисықтары бар жүйелерде үлкен криптотөзімділік анықталады, яғни зиянкестерге қандай да бір қарапайым арифметикалық операциялармен сипатталмайтын неғұрлым күрделі теңдеулерді шешу қажет болады. RSA алгоритмін бұзу кезінде зиянкестерге факторизация есебін шешуге тура келеді. Егер эллиптикалық қисықты қолданса, онда зиянкестерге дискретті логарифмді шешу керек болады, ал оның күрделілік мәселесі ECC криптоберіктігін түсіндіреді.

ӘДЕБИЕТТЕР


1. Koblitz N. Elliptic curve cryptosistems https://www.ams.org/journals/mcom/1987-48-177/S0025-5718-1987-0866109-5/S0025-5718-1987-0866109-5.pdf
2. Miller V. Uses of elliptic curves in cryptography https://link.springer.com/content/pdf/10.1007%2F3-540-39799-X_31.pdf
3. Клеменс, Г. Мозаика теории комплексных кривых. — М.: Мир, 1984.
4. Коблиц Н. Курс теории чисел и криптографии = A Course in Number Theory and Cryptography. — М.: Научное изд-во «ТВП», 2001. — С. 188—200. — 254 с.
5. Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы. — Москва: КомКнига, 2006. — 328 с.
6. Коблиц Н. Введение в эллиптические кривые и модулярные формы = Introduction to Elliptic Curves and Modular Forms. — Новокузнецк: ИО НФМИ, 2000. — 312 с.
7. L. Batina, S. B. Ors, B. Preneel, and J. Vandewalle, “Hardware architectures for public key cryptography,” INTEGRATION, the VLSI journal, vol. 34, pp. 1–64, 2003.
8. Жданов О.Н., Чалкин В.А. Эллиптические кривые: Основы теории и криптографические приложения.- М.: Книжный дом ЛИБРИКОМ, 2013.- 200с.
9. Соловьев Ю.П. и др. Эллиптические кривые и современные алгоритмы теории чисел. -Москва-Ижевск: Ин-т компьютерных исследований, 2003.



**Ақшолақ Г.И., Мағазов Р.С.**
**Научный руководитель: Дуйсебекова К.С.**


**Применение эллиптических кривых в защите информации**


**Аннотация.** Статья посвящена исследованию эллиптических кривых в криптографии. Особое внимание уделено в их преимуществе над другими криптографическими системами с открытым ключом, а также предложена платформа для аппаратной реализации эллиптической кривой в криптографии.



**Ключевые слова:** эллиптические кривые, ECC, RSA, криптосистемы с открытым ключом, платформы ASIC и FPGA.



**G.I. Aksholak, R.S. Magazov**
**Scientific superviser: Duisebekova K.S.**


**Application of elliptic curves in information protection**


**Abstract.** The article is devoted to the study of elliptic curves in cryptography. Particular attention is paid to their advantages over other public-key cryptographic systems, as well as a platform is proposed for the hardware implementation of the elliptic curve in cryptography.



**Key words:** elliptic curves, ECC, RSA, public key cryptosystems, ASIC and FPGA platforms

**Сведения об авторах:**

**Дуйсебекова Куланда Сейтбековна**, к.ф.-м.н., доцент кафедры «Информационных систем» Казахского Национального университета имени аль-Фараби.

**Ақшолақ Гүлнұр Исатайқызы**, магистрант кафедры «Информационных систем» Казахского Национального университета имени аль-Фараби.

**Мағазов Райымбек Саламатұлы**, магистрант кафедры «Информационных систем» Казахского Национального университета имени аль-Фараби.

УДК 530.1, 681.3.06

**Tukushev T.K., Kulymbetov V.A.**
International Information Technologies University
Almaty, Kazakhstan
Scientific superviser: Nurlybayev T.A.

## SECURITY IN INTERNET OF THINGS

***Abstract.*** *The Internet of things (IoT) has ceased to be a term as such. And it has become more a concept that each company interprets in its own way. IBM suggests that IoT is a set of devices that interact with each other to process data from their sensors and smart enough to transmit processed information to the Internet. Cisco represents IoT under the concept of "internet of everything", which means that any device connected to the Internet and interacts either with the user or with another device can share and process information. The Internet of things have become part of every sphere of human life. Extensive development of new IoT devices enlarges data security violation area. This article aims to analyze possible ways to harm a person's personal life by stealing personal information, as well as suggest ways to solve this problem.*

***Key words:*** *internet of things, network security, trusted platform module, regulation of digital technologies.*

### Introduction

Nowadays security in IoT devices is very low. For IoT devices, security consists primarily in the integrity of the code, authentication of users (devices), establishment of ownership (including the data generated by them), and the ability to handle virtual and physical attacks. But in fact, most of the IoT devices that are working today are not following basic security standards, they have external control interfaces, default passwords. In other words, they have all the signs of network security vulnerability.

And as practice shows, hacking in most cases is quite simple. The usual guessing of login and passwords (brute force) is enough to gain access to the device. Just a few years ago, the Mirai botnet, by selecting combinations of standard logins and passwords sewn into the factory to create them, hacked a large number of cameras and routers, which were later used for a powerful DDoS attack on the provider network UK Postal Office, Deutsche Telekom, TalkTalk, KCOM, and Eircom.

We can also recall the case of the American DNS operator DYN. The botnet attacked the devices using the device's default usernames and passwords, which led to the disconnection of almost half of the US Internet.

As you can see from these examples, hacking IoT can be even more dangerous if any of the devices are integrated into a critical infrastructure. And if we take an ordinary smart home as an example of a household level, attacks on the IoT system can lead to local communal or other emergency and dangerous situations.