ISSN 2708-2032
e-ISSN 2708-2040

INTERNATIONAL UNIVERSITY

INTERNATIONAL JOURNAL OF INFORMATION & COMMUNICATION TECHNOLOGY

Volume 1, Issue 1
March 2020

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
MINISTRY OF EDUCATION AND SCIENCE OF THE REPUBLIC OF KAZAKHSTAN

ХАЛЫҚАРАЛЫҚ УНИВЕРСИТЕТІ
МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ
INTERNATIONAL UNIVERSITY

INTERNATIONAL JOURNAL OF INFORMATION AND COMMUNICATION TECHNOLOGIES

МЕЖДУНАРОДНЫЙ ЖУРНАЛ ИНФОРМАЦИОННЫХ И КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

ХАЛЫҚАРАЛЫҚ АҚПАРАТТЫҚ ЖӘНЕ КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР ЖУРНАЛЫ

Том 1, Выпуск 1
Март 2020

Главный редактор – Ректор АО МУИТ, Заместитель главного редактора

Ускенбаева Р.К. **Дайнеко Е.А.**

ЧЛЕНЫ РЕДКОЛЛЕГИИ:

Отельбаев М. д.т.н., профессор, АО «МУИТ», Рысбайулы Б., д.т.н., профессор, АО «МУИТ», Куандыков А.А., д.т.н., профессор, АО «МУИТ», Синчев Б.К., д.т.н., профессор, АО «МУИТ», Ыдырыс А., PhD, заведующая кафедрой «МКМ», АО «МУИТ», Дузбаев Н.Т., PhD, проректор по ЦиИ, АО «МУИТ», Сербин В.В., к.т.н., заведующий кафедрой «ИС», АО «МУИТ», Шильдибеков Е.Ж., PhD, заведующий кафедрой «ЭиБ», АО «МУИТ», Айтмагамбетов А.З., к.т.н., профессор, АО «МУИТ», Амиргалиев С.Н., д.т.н., профессор, АО «МУИТ», Ниязгулова А.А., к.ф.н., заведующая кафедрой «МиИК», АО «МУИТ», Молдагулова А.Н., к.т.н., ассоциированный профессор, АО «МУИТ», Джоламанова Б.Д., ассоциированный профессор, АО «МУИТ», Prof. Young Im Cho, PhD, Gachon University, South Korea, Prof. Michele Pagano, PhD, University of Pisa, Italy, Tadeusz Wallas, Ph.D., D.Litt., Adam Mickiewicz University in Poznań, Тихвинский В.О., д.э.н., профессор, МТУСИ, Россия, Масалович А., к.ф.-м.н., Президент Консорциума Инфорус, Россия, Лусио Томмазо Де Паолис, директор-исследователь Расширенной и виртуальной лаборатории (АВР Лаб) Инженерного факультета инноваций, университет Саленто (Италия), Лиз Бэйкон, профессор компьютерных наук и заместитель проректора Университета Абертай, Великобритания

Издание зарегистрировано Министерством информации и общественного развития Республики Казахстан. Свидетельство о постановке на учет № KZ82VPY00020475 от 20.02.2020 г.

Журнал зарегистрирован в Международном центре по регистрации сериальных изданий ISSN (ЮНЕСКО, г. Париж, Франция)

Выходит 4 раза в год.

УЧРЕДИТЕЛЬ:
Международный Университет Информационных Технологий

ISSN 2708-2032 (print)
ISSN 2708-2040 (online)

I МЕЖДУНАРОДНАЯ СТУДЕНЧЕСКАЯ НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ «МОЛОДЕЖНЫЙ ЦИФРОВОЙ ФОРУМ – 2020» (YDF-2020), ПОСВЯЩЕННАЯ 10-ЛЕТИЮ МЕЖДУНАРОДНОГО УНИВЕРСИТЕТА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ПРОГРАММНЫЙ КОМИТЕТ КОНФЕРЕНЦИИ

Председатель – ректор АО МУИТ, доктор технических наук, профессор **Ускенбаева Раиса Кабиевна**

Заместитель председателя – проректор по научной и международной деятельности АО МУИТ, PhD **Дайнеко Евгения Александровна**

ЧЛЕНЫ ПРОГРАММНОГО КОМИТЕТА:

Умаров Тимур Фаридович – проректор по академической и воспитательной деятельности, PhD

Мукажанов Нуржан Какенович – декан факультета «Информационные технологии», PhD, ассистент-профессор

Дузбаев Нуржан Токкужаевич – заведующий кафедрой компьютерной инженерии и информационной безопасности, PhD, ассоциированный профессор

Сербин Василий Валерьевич – заведующий кафедрой информационных систем, кандидат технических наук, ассоциированный профессор

Шильдибеков Ерлан Жаржанович – заведующий кафедрой экономики и бизнеса, PhD, ассистент-профессор

Ниязгулова Айгуль Аскарбековна – заведующий кафедрой медиакоммуникации и истории Казахстана, кандидат филологических наук, ассоциированный профессор

Бахтиярова Елена Ажибековна – заведующий кафедрой радиотехника, электроника и телекоммуникации, кандидат технических наук, ассистент-профессор

Манапбаева Жаннура Жарканбековна – заведующий кафедрой языков

Кальпеева Жулдыз Бейшеналиевна – директор департамента по науке, PhD, ассистент-профессор

ОРГКОМИТЕТ КОНФЕРЕНЦИИ

Кальпеева Ж.Б., Арыстан Д.Б., Семенюк А.А., Молдагулова А.Н., Омаров Г.Б., Дворников А.В., Велитченко С.Н., Алипбеков А., Шетиева А.Т., Сейтнур А.М.

СОДЕРЖАНИЕ

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНЖЕНЕРИЯ ЗНАНИЙ

Shaldanbayeva N.
A generalized system for mapping relational and non-relational (NoSOL) databases..... 8
Бегарыс А.Б.
Электрондық оқу курстарын құруда iSpring suite программасын қолдану..... 11
Хажбабаев С.Р.
Разработка метода расчета коэффициента теплоотдачи многослойного искусственного сооружения..... 16
Сейтнұр А.М.
Моделирование нелинейных стационарных процессов переноса тепла в материалах.... 20
Цой Д.Д.
Виртуальная реальность как инструмент для тренировки молодых медицинских специалистов..... 23
Omirbekova Z.M.
Distribution of resources in cloud computing..... 25
Сейтнұр А.М,. Цой Д.Д., Женисов Д.К.
Разработка электронного учебника с элементами флэш-анимации..... 28
Тулеугалиев А.С.
Разработка приложения среди visual studio c# [.net] для работы с базами данных студентов..... 31
Кусаинов М.
Технологии виртуальной и дополненной реальности в инклюзивном образовании..... 34
Нұрғазиев Д.Қ., Цой Д.Д., Сейтнұр А.М.
Использавание технологии виртуальной реальности в образовании 38
Макавеев Т.А.
Миоэлектрический робототехнический экзоскелет, напечатанный на 3d принтере, для реабилитации функционирования предплечья с использованием машинного обучения..... 42
Аманкелді Н.Ғ.
C++Builder 6.0 құралдары көмегімен браузер құру..... 45
Жеңісов Д.Қ.
Разработка тестовых заданий по физике с использованием контроллера движения leap motion..... 50

ИНФОКОММУНИКАЦИОННЫЕ СЕТИ И КИБЕРБЕЗОПАСНОСТЬ

Куатова А.Б.
Сравнительный анализ оценки качества восприятия видеопотока в беспроводных каналах связи..... 53
Ақшолақ Г.И., Мағазов Р.С.
Эллиптикалық қисықтардың ақпаратты қорғауда қолданылуы 57
Tukushev T. K., Kulymbetov V.A.
Security in internet of things..... 61
Kulymbetov V.A., Tukushev T. K.
Communication protocols and security in IoT..... 65
Zhanmuratov A.
Ensuring information security of train traffic by implementing the national system ktcs on railways lines..... 68

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]:

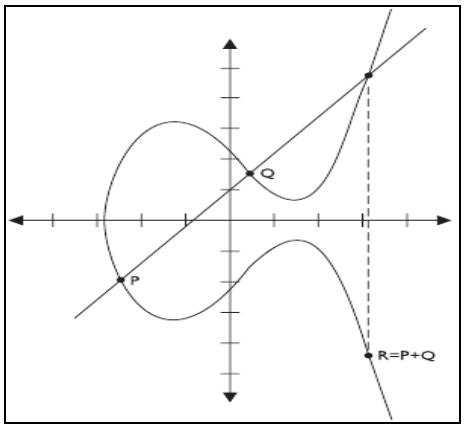
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

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: $x_{max} = \infty$, $y_{max} = \infty$.

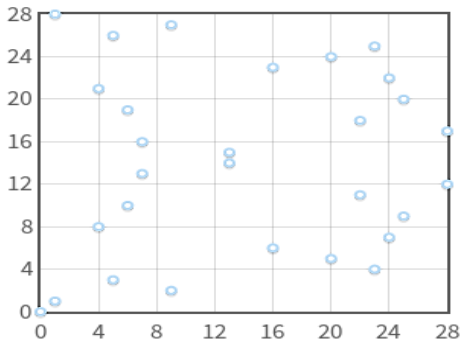
Ол кезде жоғарыда берілген теңдеу келесідей өзгереді және ол эллиптикалық криптографияда қолданылады, яғни дискретті логорифмге жүгінеміз. Криптографияда эллиптикалық қисық тек нүктелерден тұрады (2-сурет) [6].

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

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

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, ұялы 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