ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫ

әл-Фараби атындағы Қазақ ұлттық университетінің

ХАБАРЛАРЫ

ИЗВЕСТИЯ

НАЦИОНАЛЬНОЙ АКАДЕМИИ
НАУК РЕСПУБЛИКИ КАЗАХСТАН
Казахский национальный
университет имени аль-Фараби

N E W S

OF THE ACADEMY OF SCIENCES
OF THE REPUBLIC OF
KAZAKHSTAN
al-Farabi Kazakh National University

SERIES
PHYSICS AND INFORMATION TECHNOLOGY

2 (346)

APRIL – JUNE 2023

PUBLISHED SINCE JANUARY 1963

PUBLISHED 4 TIMES A YEAR

ALMATY, NAS RK

«ҚР ҰҒА Хабарлары. Физика және информатика сериясы».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Меншіктеуші: «Қазақстан Республикасының Ұлттық ғылым академиясы» РҚБ (Алматы қ.). Қазақстан Республикасының Ақпарат және қоғамдық даму министрлігінің Ақпарат комитетінде 14.02.2018 ж. берілген **No 16906-Ж** мерзімдік басылым тіркеуіне қойылу туралы куәлік.

Тақырыптық бағыты: *физика және ақпараттық коммуникациялық технологиялар сериясы.*

Қазіргі уақытта: *«ақпараттық технологиялар»бағыты бойынша ҚР БҒМ БҒСБК ұсынған журналдар тізіміне енді.*

Мерзімділігі: *жылына 4 рет.*

Тиражы: *300 дана.*

Редакцияның мекен-жайы: *050010, Алматы қ., Шевченко көш., 28, 219 бөл., тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

Типографияның мекен-жайы: «Аруна» ЖК, Алматы қ., Мұратбаев көш., 75.

«Известия НАН РК. Серия физика и информатики».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Собственник: *Республиканское общественное объединение «Национальная академия наук Республики Казахстан» (г. Алматы).*
Свидетельство о постановке на учет периодического печатного издания в Комитете информации Министерства информации и общественного развития Республики Казахстан **No 16906-Ж** выданное 14.02.2018 г.
Тематическая направленность: *серия физика и информационные коммуникационные технологии.*
В настоящее время: *вошел в список журналов, рекомендованных ККСОН МОН РК по направлению «информационные коммуникационные технологии».*
Периодичность: *4 раз в год.*
Тираж: *300 экземпляров.*
Адрес редакции: *050010, г. Алматы, ул. Шевченко, 28, оф. 219, тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

Адрес типографии: ИП «Аруна», г. Алматы, ул. Муратбаева, 75.

News of the National Academy of Sciences of the Republic of Kazakhstan.
Series of physics and informatics.
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Owner: RPA «National Academy of Sciences of the Republic of Kazakhstan» (Almaty). The certificate of registration of a periodical printed publication in the Committee of information of the Ministry of Information and Social Development of the Republic of Kazakhstan **No. 16906-Ж,** issued 14.02.2018
Thematic scope: *series physics and information technology.*
Currently: *included in the list of journals recommended by the CCSES MES RK in the direction of «information and communication technologies».*
Periodicity: *4 times a year.*
Circulation: *300 copies.*
Editorial address: *28, Shevchenko str., of. 219, Almaty, 050010, tel. 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

Address of printing house: ST «Aruna», 75, Muratbayev str, Almaty.

NEWS OF THE NATIONAL ACADEMY OF SCIENCESOF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES
ISSN 1991-346X
Volume 2. Namber 346 (2023). 261-273
https://doi.org/10.32014/2023.2518-1726.198

МРНТИ 81.93.29
УДК 004.056.5

© G.K. Shametova[1*], A.A. Sharipbay[2], B.G. Sailau[1], 2023
[1]Al-Farabi Kazakh National University, Almaty, Kazakhstan;
[2]L.N. Gumilyov Eurasian National University, Astana, Kazakhstan.
E-mail: gauharshametova@gmail.com

ANALYSIS OF CRYPTOGRAPHIC SECRET DISTRIBUTION SCHEMES IN ACCESS CONTROL SYSTEMS

Shametova Gauhar Kuttymuratqyzy — Doctoral student of the Department of Information Systems of the Al-Farabi Kazakh National University, Almaty, Kazakhstan
E-mail: gauharshametova@gmail.com;
Sharipbay Altynbek Amiruly — Candidate of Physical and Mathematical Sciences, Doctor of Technical Sciences, L.N.Gumilyov Eurasian National University, Astana, Kazakhstan
E-mail: sharalt@mail.ru, https://orcid.org/0000-0001-5334-1253;
Sailau Baglan Galymzhanuly — Doctoral student of the Department of Information Systems of the Al-Farabi Kazakh National University, Almaty, Kazakhstan
E-mail: baglan.13.bs@gmail.com.

Abstract. In the modern world, a large amount of information is stored and processed in the information systems of organizations that require protection with secret keys. In most places, various passwords, PIN codes, etc. are used as keys. In case of their loss, access to information systems may also be lost. Therefore, the tasks of safe storage or recovery of basic information are relevant. The article discusses the main methods of solving problems related to the loss and recovery of keys: creating a backup copy and storing it in different places; reliable key storage by several subscribers; use of cryptographic secret distribution protocols. It is established that the most effective solution to the problem under consideration is the use of cryptographic secret distribution protocols. These protocols provide for modern types of computer attacks. This article also analyzes the limit schemes of secret distribution, which are the basis of cryptographic secret separation protocols. The analysis of limit schemes is carried out on the basis of the following parameters: perfection, ideality, resource consumption, evaluation of the complexity of algorithmic calculation. It was found that Shamir's limit scheme is ideal and requires fewer resources compared to other options. Therefore, it can be recommended as a suitable option for solving problems with saving and restoring the secret key.

Keywords: secret distribution schemes, key, key distribution, key recovery, edge cryptography, Shamir scheme

© Г.Қ. Шаметова[1*], А.Ә. Шәріпбай[2], Б.Ғ. Сайлау[1], 2023
[1]Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан;
[2]Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан.
E-mail: gauharshametova@gmail.com

ҚОЛЖЕТІМДІЛІКТІ БАСҚАРУ ЖҮЙЕЛЕРІНДЕГІ ҚҰПИЯНЫ БӨЛУДІҢ КРИПТОГРАФИЯЛЫҚ СҰЛБАЛАРЫН ТАЛДАУ

Шаметова Гауһар Құттымұратқызы — Әл-Фараби атындағы Қазақ ұлттық университетінің Ақпараттық жүйелер кафедрасының докторанты, Алматы, Қазақстан
E-mail: gauharshametova@gmail.com;
Шәріпбай Алтынбек Әміруұлы — Физика-математика ғылымдарының кандидаты, техника ғылымдарының докторы, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан
E-mail: sharalt@mail.ru, https://orcid.org/0000-0001-5334-1253;
Сайлау Бағлан Ғалымжанұлы — Әл-Фараби атындағы Қазақ ұлттық университетінің Ақпараттық жүйелер кафедрасының докторанты, Алматы, Қазақстан
E-mail: baglan.13.bs@gmail.com.

Аннотация. Қазіргі заманда ұйымдардың ақпараттық жүйелерінде құпия кілттермен қорғауды қажет ететін үлкен көлемді ақпараттар сақталады және өңделеді. Көп жерде кілт ретінде әртүрлі құпия сөздер, пин-кодтар және т.б. қолданылады. Олар жоғалған жағдайда ақпараттық жүйелерге қолжетімділік те жоғалуы мүмкін. Сондықтан кілттерді қауіпсіз сақтау немесе қалпына келтіру міндеттері өзекті болып табылады. Мақалада кілттерді жоғалтуға және қалпына келтіруге байланысты мәселелерді шешудің негізгі әдістері қарастырылған: резервті көшірме жасау және оны әр түрлі жерлерде сақтау; бірнеше абоненттің кілттерді сенімді сақтауы; құпияны криптографиялық бөлу хаттамаларын қолдану. Қарастырылып отырған мәселенің ең тиімді шешімі құпияны криптографиялық бөлу хаттамаларын қолдану болып табылатыны анықталды. Осы хаттамаларға компьютерлік шабуылдардың заманауи түрлері қарастырылған. Сондай-ақ, бұл мақалада құпияны криптографиялық бөлу хаттамаларының негізі болып табылатын құпияны бөлудің шекті сұлбалары талданады. Шекті сұлбаларды талдау келесі параметрлер негізінде жүзеге асырылады: жетілдіру, идеалдылық, ресурстарды тұтыну, алгоритмді есептеудің күрделілігін бағалау. Шамирдің шекті сұлбасы басқа нұсқалармен салыстырғанда мінсіз және ресурстарды аз қажет ететіні анықталды. Сондықтан оны құпия кілтті сақтау және қалпына келтіру мәселелерін шешудің қолайлы нұсқасы ретінде ұсынуға болады.

Түйін сөздер: құпияны бөлу сұлбалары, кілт, кілттерді бөлу, кілтті қалпына келтіру, шекті криптография, Шамир сұлбасы

© Г.Қ. Шаметова[1*], А.Ә. Шәріпбай[2], Б.Ғ. Сайлау[1], 2023
[1]Казахский национальный университет им. аль-Фараби, Алматы, Казахстан;
[2]Евразийский национальный университет им. Л.Н. Гумилева,
Астана, Казахтан.
E-mail: gauharshametova@gmail.com

АНАЛИЗ КРИПТОГРАФИЧЕСКИХ СХЕМ РАСПРЕДЕЛЕНИЯ СЕКРЕТОВ В СИСТЕМАХ УПРАВЛЕНИЯ ДОСТУПОМ

Шаметова Гаухар Куттымураткызы — Докторант кафедры информационных систем Казахского национального университета имени Аль-Фараби, Алматы, Казахстан
E-mail: gauharshametova@gmail.com;
Шарипбай Алтынбек Амирулы — Кандидат физико-математических наук, доктор технических наук, Евразийский национальный университет им. Л.Н. Гумилева, Астана, Казахстан
E-mail: sharalt@mail.ru, https://orcid.org/0000-0001-5334-1253;
Сайлау Баглан Галымжанулы — Докторант кафедры информационных систем Казахского национального университета имени Аль-Фараби, Алматы, Казахстан
E-mail: baglan.13.bs@gmail.com.

Аннотация. В современном мире в информационных системах организаций хранится и обрабатывается большой объем информации, требующей защиты секретными ключами. В большинстве мест в качестве ключей используются различные пароли, пин-коды и т.д. В случае их утраты также может быть потерян доступ к информационным системам. Поэтому задачи безопасного хранения или восстановления основной информации актуальны. В статье рассмотрены основные методы решения проблем, связанных с потерей и восстановлением ключей: создание резервной копии и ее хранение в разных местах; надежное хранение ключей несколькими абонентами; использование протоколов криптографического распределения секретов. Установлено, что наиболее эффективным решением рассматриваемой проблемы является использование протоколов криптографического распределения секретов. В этих протоколах предусмотрены современные виды компьютерных атак. В этой статье также анализируются предельные схемы распределения секретов, которые являются основой протоколов криптографического разделения секретов. Анализ пороговых схем осуществляется на основе следующих параметров: совершенство, идеальность, расход ресурсов, оценка сложности алгоритмического расчета. Было обнаружено, что пороговая схема Шамира идеальна и требует меньше ресурсов по сравнению с другими вариантами. Поэтому его можно рекомендовать как подходящий вариант для решения проблем с сохранением и восстановлением секретного ключа.

Ключевые слова: схемы распределения секретов, ключ, распределение ключей, восстановление ключей, краевая криптография, схема Шамира

Кіріспе

Қоғам дамуының қазіргі кезеңі ақпараттық саланың өсіп келе жатқан рөлімен сипатталады. Қазақстан Республикасының ұлттық қауіпсіздігі ақпараттық қауіпсіздікті (АҚ) қамтамасыз етуге айтарлықтай тәуелді және болашақта бұл тәуелділік тек артады (Писковаг 2015) Сондықтан қауіпсіз цифрлық кеңістікті қамтамасыз ету үшін ақпаратты қорғау әдістеріне (технологияларына) қатысты мәселелер өте маңызды. Көбінесе мұндай сұрақтар ақпараттық ресурстарға ұжымдық қол жеткізуді шектеудің күрделі міндеттеріне әкеледі. Ұйымдардың барлық заманауи ақпараттық жүйелерінде дерлік мәліметтердің үлкен көлемі сақталады және өңделеді, оларды қорғау кілттерді пайдалануды көздейді. Көбінесе құпиялар әкімшілік қол жеткізуге арналған құпия кілттер, парольдер, кодтық сөздер, құпия және т.б. Бұл ретте құпия кілт деректердің құпиялылығын қамтамасыз етеді, ал егер ол жоғалса, ақпараттық жүйелерге қол жеткізу жоғалуы мүмкін. Осыған сүйене отырып, құпия кілт жоғалған жағдайда негізгі АЖ қызметтерінің бірі — «қолжетімділік» — көрсету қажеттілігі туындайды. Сондықтан, осы мақаланың негізгі мақсаты — құпия кілт қауіпсіз сақталуын қамтамасыз етуге және қажет болған жағдайда оны қалпына келтіруге қатысты мәселелерді кешенді талдау. Пәндік аймақтың жалпы сипаттамасы. Мақалада қарастырылған мәселені шешудің әртүрлі жолдары бар (ақпараттық қауіпсіздіктің қажетті стандарттарына сәйкес құпия кілт қалпына келтіру мүмкіндігін қамтамасыз ету): негізгі ақпараттың сақтық көшірмесін жасау және әртүрлі жерлерде көшірмелерді сақтау; бірнеше абоненттің кілтті құпия түрде беруі; криптографиялық құпияны ортақ пайдалану протоколдарын (ККОПП) пайдалану. Дегенмен, бұл әдістердің әрқайсысының белгілі бір кемшіліктері бар. Өзара олар салыстырылды, нәтижелері 1-кестеде берілген.

Кесте 1. Құпия кілтті резервтік сақтау әдістерінің салыстырмалы талдауы

Параметр	Резервтік көшірмені пайдалану	Кілттерді бірнеше жазылушыларға сену	Құпияны криптографиялық бөлу хаттамаларын қолдану
Қарапайымдылық	+	+	–
Сенімділік	+	–	+
Сенімділік	–	–	+
Құпиялылық	–	–	+

1-кестедегі деректерді талдау негізінде құпия кілт жоғалған жағдайда ақпараттың қолжетімділігі мен құпиялылығын қамтамасыз етудің ең тиімді жолы деректерді таратылған сақтау үшін қолданылатын ККОПП пайдалану болып табылатынын көруге болады.

ККОПП жұмыс істеу принципін түсіну үшін құпия бөлісу хаттамаларын қолданудың демонстрациялық мысалын қарастырайық. Ақпараттық жүйенің (АЖ) ақпараттық қауіпсіздік әкімшісі төрт қызметкер арасында он екі таңбадан

тұратын құпия кілт бөлісуі керек делік. Бұл қандай да бір себептермен АЖ әкімшісі болмаған жағдайда қызметкерлер АЖ-ға жылдам қол жеткізуі және қажетті шұғыл операцияларды орындауы үшін қажет.

Бұл жағдайда АЖ әкімшісі дилер (бөлуші), ал қызметкерлер кастодиан болып табылады. Сипатталған технологияға (тәсілге) сандық мысал келтірейік. Құпия z@far2190429 таңбалар тізбегі болсын. Құпия бөлісу: 1-ші қызметкер үшін «429» белгілері және № 4 лауазымы; 2-ші қызметкерге «ar2» таңбалары тобы үшін № 2 лауазымы; 3-ші қызметкерге "z@f" белгілері және № 1 лауазымы; 4-ші қызметкер үшін «190» белгілері және № 3 лауазымы. Бұл тәсілдің елеулі кемшілігі — құпияның бөліктерін қызметкерлер ашық түрде сақтайды. Бұл факт ақпараттың құпиялылық деңгейіне айтарлықтай әсер етеді.

Осы кемшілікке байланысты қарастырылған құпияны бөлісу технологиясы іс жүзінде «жұмыс» мақсаттары үшін пайдаланылмайды. Оны жақсарту негізінен, мысалы, криптографиялық түрлендірулерді қолдану арқылы мүмкін. Бұл технология ККОПП деп аталады. Дегенмен, ақпараттық технологиялардың қарқынды дамуына байланысты ККОПП қауіпсіздігі төмендеді, өйткені осы хаттамаларды бұзуға бағытталған компьютерлік шабуылдардың жаңа түрлері пайда болды. Атап айтқанда, бұл Positive Technologies жүргізген талдау нәтижелеріне сәйкес, ақпараттық жүйелерде құпия сөздерді сақтау кезінде көп жағдайда оларды жергілікті сақтау/қалпына келтіру үшін қорғаныс механизмдері қолданылмайды. Сондықтан оларды жетілдіру мақсатында ККОПП талдау өте өзекті міндет деп айтуға болады.

Материалдар мен зерттеу әдістері

Кез келген криптографиялық хаттама ақпараттық процестерде криптографиялық түрлендірулер мен алгоритмдерді қолдануды реттейтін нақты ережелер жиынтығына негізделген. ККОПП шекті құпияны бөлу сұлбасы (ҚБС) алгоритміне негізделуі мүмкін.

Типтік жағдайларда ККОПП екі негізгі фазаны қамтиды.

1. Құпия бөлу – М құпиясын білетін дилер (бөлуші) $c_1, c_2, ..., c_n$ құпияның n үлесін тудыратын және қорғалған байланыс арнасы арқылы әрбір қатысушыға оның үлесін беретін тарату кезеңі. Тарату заңды абоненттер бірлескен іс – әрекеттер кезінде ғана құпияны қалпына келтіре алатындай, ал заңсыз абоненттер мүмкін болмайтындай етіп ұйымдастырылады.

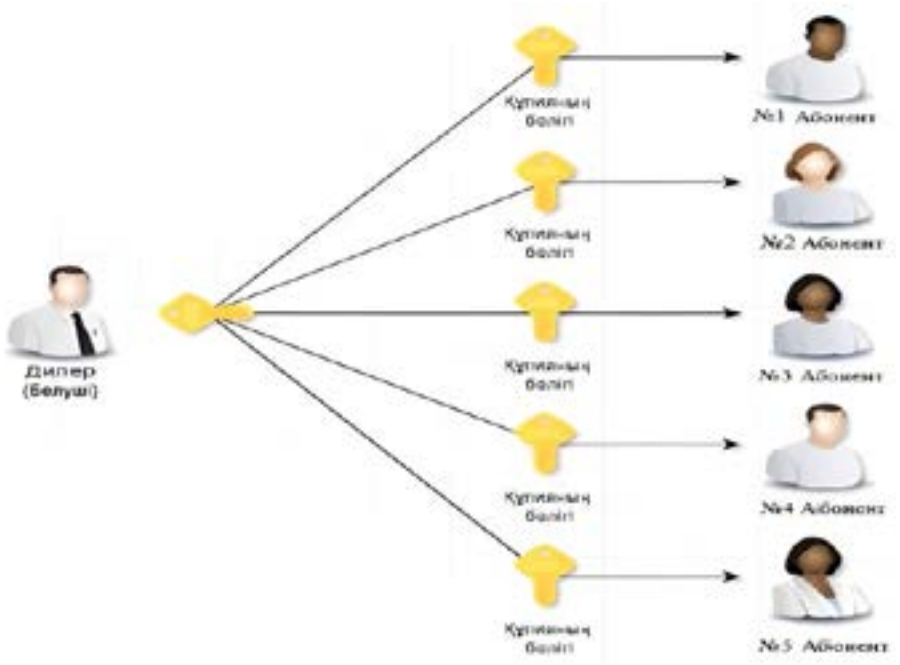
2. Құпияны қалпына келтіру-заңды абоненттер өздерінің құпия үлестерін біріктіріп, құпияны ала алатын кезең. Бұдан әрі қарастырылатын алгоритмдердің көпшілігінде "құпия" ақпарат бөлінген барлық заңды абоненттерді қалпына келтіруге міндетті қатысу қажет.

Суретте құпияны бөлудің шекті сұлбасы көрсетілген.

Зерттеу барысында келесі шекті ҚБС қарастырылды:

- Шамир ҚБС;
- Блэкли ҚБС;

- Эллиптикалық қисыққа негізделген ҚБС;
- Карнин-Грин-Хеллман Қ БС ;
- Асмут – Блум ҚБС.



Сур.1. Классикалық құпияны бөлісу хаттамасының сұлбасы
(*Fig.1.* Outline of the classic secret sharing protocol)

Ең тиімді ККОПП анықтау үшін алгоритмдерді қолданудың қауіпсіздік деңгейіне әсер ететін келесі негізгі параметрлер бойынша олардың салыстырмалы талдауын жүргізу туралы шешім қабылданды:

1) есептеулердің күрделілігі. Алгоритмнің күрделілігін бағалау құпияны бөлісу және қалпына келтіру кезеңінде алынған бағалаулардан тұрады;

2) есептеу ресурсының қарқындылығы (құпияны ортақ пайдалану және қалпына келтіру кезеңдерінде пайдаланылатын жад көлемі);

3) кемелдік (егер заңсыз пайдаланушылардың кез-келген саны құпия туралы ешқандай ақпарат ала алмаса, ҚБС мінсіз болады);

4) идеалдылық (егер құпияның үлесінің мөлшері құпияның өзіне тең болса, ҚБС өте қолайлы).

Бұл жұмыста келесі белгілер қолданылады:

k – құпияны қалпына келтіру үшін қажетті заңды абоненттердің ең аз саны;

n – құпия бөлінетін үлестер саны;

p – үлкен жай Сан;

Z_p – бүтін сандардың қарапайым сақина Модулінің өлшемі;

M – құпия (кілт).

Шамир құпиясының бөлу сұлбасы. Шамир шекті сұлбасы (*k, n*) көпмүшелік интерполяция ұғымы төңірегінде құрылған. Егер құпияны тек k абонент қалпына келтіре алатындай етіп бөлу қажет болса, онда оны (*k-1*) дәрежелі көпмүшелік формуласында «жасыру» керек. Бұл көпмүше *k* нүктелері бойынша қалпына келтіріледі. Есептеулердің күрделілігін талдап көрейік.

Құпияны бөлу кезеңі.

1-қадам. Бұл қадамда p кездейсоқ жай саны таңдалады. Санның қарапайымдылығын тексеру ресурсты көп қажет ететін процесс және алгоритмнің күрделілігін жалпы бағалауға айтарлықтай әсер етеді. Бұл қадамды бағалау санның қарапайымдылығын тексеру үшін қолданылатын алгоритмге байланысты. Қарапайымдылығын тексеру үшін

кездейсоқ таңдалған сан Бей және – Померанц – Селфридж – Вагстафф ықтималдық сынағы пайдаланылды (Chervyakov, 2016). Бұл қадамның күрделілігі O (1) – (Молдовянғ 2011) ден алынған орташа мәнге тең.

2-қадам. Өріс үстінде көпмүшені құру алгоритмінің осы қадамында

Z_p , *(k-1)* коэффициенттерін таңдайды. Қадамның күрделілігін бағалау O(k) тең.

3-қадам. Көлеңкелерді есептеуге арналған қайталанулар саны n-ге тең, әрбір итерация *(k–1)* координаттар бойынша өтетін кірістірілген циклды қамтиды. Берілген қадамның жалпы бағасы *O(k·n)*.

$k < n < k$ болғандықтан, құпияны бөлу үшін есептеулердің күрделілігін бағалау *O(k·n)* болады. Құпияны қалпына келтіру кезеңі. Құпияны қалпына келтіру процесі Лагранж интерполяциялық көпмүшесін құру арқылы жүзеге асырылады. Алгоритмнің күрделілігінің жалпы бағалау $O(k \cdot n)+O(k^2)$.

Есептеулердің ресурс сыйымдылығын талдау. Құпия фракцияларды сақтауға арналған жедел жад құрылғысының қажетті жады мөлшері $n \cdot |M| + O(|m|)$ мәніне тең, мұндағы

$| m |$ - құпияның максималды ұзындығы М. құпияны бөлу/қалпына келтіру үшін

$n = k = 64$ кезінде шамамен 8192 байт жедел жады қажет болады.

Кемелдік/идеалдық. Шамирдің сұлбасы кемелді және идеалды. Идеалдылық құпияның өлшемі p өлшеміне, сондай-ақ әрбір қатысушының құқығы бар құпияның үлесіне тең болуынан туындайды. Шамир сұлбасындағы құпия сызықтық теңдеулер жүйесін шешу арқылы қалпына келтірілді делік. Заңсыз жазылушылар *k* белгісізі бар *k* кем теңдеулер жүйесін құруы керек. Мұндай жүйенің шешімі *k*-өлшемді кеңістіктегі гипержазықтықта жатқан нүктелер жиыны болып табылады, бұл ешқандай құпия мәнді мүмкін емес деп жоққа шығаруға болмайтынын білдіреді. Сондықтан Шамирдің сұлбасы мінсіз.

Блэклидің құпия бөлісу сұлбасы. Блэкли сұлбасы немесе векторлық ҚБС көп өлшемді кеңістікте нүктелерді пайдалануға негізделген. Кез келген екі немесе одан да көп жазықтық кеңістікте қиылысады, ал қиылысу нүктесінің

координаттарының бірі құпия болып табылады. Егер құпия нүктенің бірнеше координаттары ретінде кодталса, онда бір гипержазықтықтан құпия туралы, яғни қиылысу нүктесінің координаталарының өзара тәуелділігі туралы кейбір мәліметтерді алуға болады. Есептеулердің күрделілігін талдап көрейік.

Құпия бөлісу кезеңі.

1-қадам. Шамир сұлбасындағыдай, бұл қадамның күрделілік бағасы санның қарапайымдылығын тексеру алгоритміне байланысты және *O(1)* болады.

2-қадам. *(k–1)* сандарды таңдау кезіндегі бұл қадамның күрделілігі *O(k)* болады.

3-қадам. n қатысушының әрқайсысы үшін di коэффициенті анықталады және әрбір итерацияда кездейсоқ құрылған k санының жиынтығы қажет. Қадамның есептеу күрделілігін бағалау *O(k·n)* болады.

4-қадам. Шамир сұлбасындағыдай, құпияның үлесін n қатысушымен бөлісу үшін *n* қайталану қажет. *O(n)* уақытында қатысушыларға құпияның үлестері беріледі.

Қалпына келтіру кезеңі. Құпияны қалпына келтіру тапсырмасы сызықтық теңдеулер жүйесін шешу арқылы жүзеге асырылады. Мұндай шешімнің тиімді нұсқасы Крамер әдісін қолдану болып табылады, өйткені құпия шешім нәтижесінде алынған нүктенің бірінші координатасы болып табылады.

Құпияны қалпына келтіру үшін $k \cdot k$ өлшемі бар матрицалардың екі анықтауышын есептеу керек.

Матрицалық анықтауыштар Гаусс әдісі негізінде анықталады, ал күрделілік бағасы $O(k^3)$.

Блэкли тізбегінің есептеу күрделілігінің жалпы бағасы $O(k \cdot n)+O(k^3)$ болып табылады.

Есептеулердің ресурс қарқындылығын талдау. Құпияны үлестерге бөлуге қажетті жедел жадының байт саны $n \quad k \quad |m|$ ретінде бағаланады. $n = k = 64$ құпия бөлісу/қалпына келтіру операциялары үшін шамамен 266 Кбайт жедел жады қажет болады.

Кемелдік/идеалдық. Құпиядағы әрбір үлестің мөлшері құпияның өлшемінен *k* есе көп болғандықтан, Блэклидің сұлбасы мінсіз болуы мүмкін емес. Дегенмен, бұл кемелді , өйткені *k* белгісізі бар *(k–1)* сызықтық салыстырулар жүйесінің шешімі *k* өлшемді кеңістіктегі гипержазықтықта жатқан шешімдер жиыны болып табылады. Бұл құпия *M* мүмкін болатын құпиялар жиынынан кез келген мәнді қабылдай алатынын білдіреді.

Эллиптикалық қисыққа негізделген құпия бөлісу сұлбасы. Эллиптикалық қисық бойынша құпияның бөлінуі төменде сипатталған алгоритміне сәйкес жүреді. Есептеулердің күрделілігін талдап көрейік.

Бөлу кезеңі.

1-қадам. Дилер қажетті нүктелер саны (кемінде n) бар EC эллиптикалық қисығын таңдайды. ҚБС қатысушыларының әрқайсысына (соның ішінде

құпия сақтаушы) эллиптикалық қисықтағы нүкте, оның ішінде «шексіз қашықтағы» нүкте беріледі.

2-қадам. Бұл қадамда дилер осы қисық бойынша n дәрежелі көпмүшені таңдайды. Бұл көпмүшенің коэффициенттері оған ғана белгілі. Эллиптикалық қисықтағы қатысушы — құпияны сақтаушыны білдіретін нүкте бәріне белгілі.

3-қадам. Дилер осы нүктенің координаталарын өзі таңдаған көпмүшеге ауыстырады, құпияның мәнін есептейді.

4-қадам. Әрбір қатысушыға құпияның өз үлесін беру үшін дилер ол үшін құпия үлесін ала отырып, қатысушы нүктесінің координаталарын көпмүшеге ауыстырады. Нәтижесінде қатысушының эллиптикалық қисықтағы нүктесі (ID) және құпияның үлесі (Secret) болады.

Эллиптикалық қисықтарға негізделген сұлбалардағы құпияны бөлісу фазасының есептеу күрделілігінің жалпы мағынасы $O(k \cdot n)$-ге тең.

Қалпына келтіру кезеңі. Құпияны қалпына келтіру үшін дилер таңдаған көпмүшенің коэффициенттерін қалпына келтіру үшін бірнеше қатысушылар бірігуі керек. Математикалық тұрғыдан бұл кейбір теңдеулер жүйесін шешуге дейін азайтады. Рұқсат етілген коалицияны құрайтын қатысушылар қажетті көпмүшені алады. Олар оған құпияны білдіретін нүктенің координаталарын қояды. Нәтижесінде олар дилер қалыптастырған құпияны алады. Бұл сұлбадағы құпия қалпына келтіру кезеңінің есептеулерінің есептік күрделілігі $O(k^2)$.

Есептеулердің ресурс қарқындылығын талдау. Эллиптикалық қисық сызықтағы нүктенің оперативті жады мөлшері құпияның өзін сақтауға қажетті мөлшерден аспайтындықтан, сұлба Шамир сұлбасының ресурс қарқындылығын сақтап алады.

Құпияны қалпына келтіру үшін сізге шамамен 25 Кбайт жад қажет.

Кемелдік/идеалдық. Эллиптикалық қисықтарға негізделген сұлбалар кемелді болып табылады, өйткені заңсыз пайдаланушылардың құпия фракцияларында құпия туралы ешқандай ақпарат болмайды. Алайда, олар идеалды емес, өйткені құпияның әрбір үлесінің мөлшері құпиядан k есе көп.

Карнин-Грин-Хеллман құпиясымен бөлісу. Бұл сұлба алгебралық теңдеулер жүйесін шешуге негізделген. Есептеулердің күрделілігін талдап көрейік.

Бөлу кезеңі.

Құпияны n түрлі тарап (топ мүшелері) арасында бөлісу үшін, кем дегенде k тарап оны қалпына келтіре алатындай, k өлшемінің $(n+1)$ V_i векторлары таңдалады, сонымен қатар берілген k вектордан тұратын кез келген матрицаның рангі k-га тең болуы қажет. V_0 векторы барлық қатысушыларға белгілі. Құпия ішкі туынды болып табылады (u, V_0), мұндағы u — векторлар жиыны, ал бөліктері - ішкі туындылар (u, Vi). Құпияны n бөлікке бөлу қадамының күрделілігі $O(n)$-ге тең.

Қалпына келтіру кезеңі. Белгілі үлестер бойынша құпияны қалпына келтіру үшін u векторын табу үшін k теңдеулерінің жүйесі шешіледі.

Есептеулердің ресурс сыйымдылығын талдау. Құпия 2 вектордың матрицалық көбейтіндісі түрінде ұсынылғандықтан, векторлардың координаттарын сақтауға арналған жедел жад көлемі 64 байтқа тең. N = 64 кезінде құпияны бөліктерге бөлу үшін сізге $(2 \cdot n+1) \cdot 64 = 8256$ байт жедел жады қажет етеді.

Құпияны қалпына келтіру үшін сызықтық алгебралық теңдеулер жүйесін шешу қажет. Бүтін арифметиканың ең жақсы нұсқасы Крамер әдісі болып табылады. Мәнді есептеу үшін $k \times k$ өлшемі бар матрицалардың $(k+1)$ анықтауыштарын алу керек. Нәтижесінде құпияны қалпына келтіру үшін 8320 байт жедел жады қажет болады.

Кемелдік/идеалдық. Карнин-Грин-Хеллман сұлбасы кемелді болып табылады, өйткені құпия M ықтимал құпиялар жиынтығынан кез келген мәнді қабылдай алады. Алайда, ол эллиптикалық қисық сызықтарға негізделген сұлба сияқты идеалды емес, өйткені құпияның әрбір үлесінің мөлшері құпияның өзінен k есе көп.

Асмут-Блум құпиясын бөлісу сұлбасы. Асмут-Блум сұлбасы — жай сандарды пайдаланып құрастырылған шекті құпияны бөлісу сұлбасы. Құпияны кез келген k қатысушы қалпына келтіре алатындай етіп n тарап арасында бөлісуге мүмкіндік береді. Есептеулердің күрделілігін талдап көрейік.

Бөлу кезеңі.

1-қадам. (k, n) шекті сұлба үшін p жай саны таңдалады.

2-қадам. Содан кейін Асмут-Блум шарттары орындалатын $p - d_1, d_2, \ldots, d_n$ мәнінен кіші сандар таңдалады.

Құпия бөлісу кезеңінің есептік күрделілігі $O(n)$ болып табылады.

Қалпына келтіру кезеңі. Қытайлық қалдық теоремасын пайдалана отырып, кез келген k құпия үлестерді біріктіру арқылы құпияны қалпына келтіруге болады, бірақ бұл кез келген (k-1) құпия үлестермен мүмкін емес (Kiparisova, 2016). Құпия қалпына келтіру кезеңінің есептеулерінің күрделілігі $O(k^2)$-ге тең.

Есептеулердің ресурс қарқындылығын талдау. Әрбір жай сан d_i 100 байт оперативті жадты алады. Содан кейін d_j табу шарттарын тексеру үшін 2^k $|d_i|$ есте сақтау, яғни. шамамен 12,8 КБайт. Жадта құпияның бір үлесін сақтау үшін p = 28 байт, k = 64 байт, $|p|+|d_i|+|k_i|$ шамамен 192 байтты құрайды. Нәтижесінде құпияны бөлісу үшін 57 Кбайт жедел жады қажет болады. Құпияны қалпына келтіру үшін шамамен 320 байт қажет.

Кемелдік/идеалдық. Асмут-Блум сұлбасы кемелді, себебі M құпиясы мүмкін болатын құпиялар жиынтығынан кез келген мәнді қабылдай алады. Бірақ бұл да идеалды емес, өйткені құпияның әрбір үлесі құпияның өзінен k есе көп.

Осы уақытқа дейін мақалада ресурстардың қарқындылығы мен есептеу күрделілігі тұрғысынан шекті ҚБС талданды. Сондай-ақ, осы сұлбаларға

шабуыл түрлерін қарастыру маңызды, өйткені ғылыми-техникалық прогреске байланысты бұзушылар шабуылдардың барған сайын жетілдірілген түрлерін ойлап табады (қолданады).

Шекті құпияны бөлісу сұлбаларына шабуыл түрлері. Егер зиянкес құпия бөлісуге қатысушылардың *k* санына еніп кетсе, шекті ҚБС-на компьютерлік шабуыл жасалуы мүмкін.

Зиянкестің шекті сұлбаны айналып өтуге көптеген әлеуетті мүмкіндіктері бар. Атап айтқанда, мынаны қарастырып өтеміз.

1. Шабуылдаушы құпияның дұрыс емес бөлігін (мысалы, ерікті санды) әдейі пайдалана алады - бұл жағдайда топ құпияны қалпына келтіре алмайды. Дегенмен, дұрыс емес бөлікті кім ұсынғанын анықтау мүмкін емес.

2. Егер шабуылдаушы өзін қатысушы етіп көрсете алса , құпия бөлісу процедурасының басталуына себеп болуы мүмкін. Содан кейін ол қалған қатысушылардың құпиясының үлесін ала алады.

3) *(k; n)* шекті сұлбада құқық бұзушы өзін *(k+1)* қатысушы ретінде көрсете алады. Құпияны қалпына келтіру үшін *k* қатысушы жеткілікті болғандықтан, шабуылдаушы құпияның өз үлесі ретінде таңбалардың ерікті тізбегін ұсына алады.

Бұл жағдайда бұзушы басқа заңды абоненттердің құпиясының бөліктерін біліп, содан кейін құпияны толығымен қайта жасай алады. Бұл кейбір ҚБС-ның жетілмегендігінің салдары.

Сондай-ақ, бұзушы жұмыс уақытынан, кэштеуден, қосымшаның істен шығуынан және т.б. пайдалы ақпаратты алуға тырысқанда, сыртқы арналар арқылы ҚБС-на компьютерлік шабуылдардың қаупі бар. Мұндай шабуылдарды жүргізу мүмкіндігі әдетте бағдарламалық жасақтаманы әзірлеу кезінде жіберілген қателермен байланысты.

Нәтижелер

Жүргізілген зерттеу нәтижелері ККОПП қолдану негізгі ақпаратты сақтаудың/қалпына келтірудің ең тиімді әдісі екенін көрсетті. Сондай-ақ, ККОПП ақпараттық қауіпсіздік деңгейіне айтарлықтай әсер ететін компьютерлік шабуылдардың заманауи түрлеріне бейім екендігі анықталды.

2-кестеде құпияны бөлудің шекті сұлбаларын салыстырмалы талдау нәтижелерінің қысқаша мазмұны көрсетілген.

Кесте 2. Шекті ҚБС салыстырмалы талдау нәтижелері

Шекті сұлба	Кемел-дік	Идеал-ды	Ресурс сыйымдылығы (Кбайт)	Қиындықты бағалау
Шамир сұлбасы	+	+	8	$O(n \cdot k)+O(k^2)$
Блэкли сұлбасы	+	–	266	$O(n \cdot k)+O(k^3)$
Эллиптикалық қисыққа негізделген сұлбасы	+	–	25	$O(n \cdot k)+O(k^2)$
Карнин-Грин-Хеллман сұлбасы	+	–	8,1	$O(n)+O(k^3)$
Асмут – Блум сұлбасы	+	–	57	$O(n)+O(k^2)$

2-кестеден Шамир сұлбасы кемелдік пен идеалдылық қасиеттеріне ие, ол басқа сұлбалармен салыстырғанда ресурстарды аз қажет етеді деген қорытынды жасауға болады. Есептеулердің күрделілігі бойынша Шамир сұлбасы Асмут-Блум сұлбасынан төмен. Алайда, бұл жағдайда басқа параметрлердің артықшылығы шешуші болып табылады.

Қорытынды

Шекті құпияны бөлісу сұлбаларын салыстырмалы талдау нәтижелері Шамир сұлбасы ҚБС көрсеткіштерінің кешені бойынша қалғандарымен салыстырғанда ең тиімді болып табылатындығын көрсетеді. Сондықтан бұл сұлбаны қорғалған ККОПП-ті кеңіннен дамыту үшін негіз ретінде қолданған жөн. Осы зерттеу нәтижесінде қол жеткізуді басқару жүйесі үшін шекті криптографияны пайдаланып, құпия кілттерді бөлудің жаңа әдісін әзірлеу, ал ҚБС ретінде Шамир сұлбасын пайдалану жоспарланып отыр.

REFERENCES

Alferov A.P. et al., 2005. Osnovy kriptografii : uchebnoe posobie [Basics of cryptography : Tutorial]. 3-rd ed., rev. and add. Moscow, Gelios ARV Publ., 2005. 480 p. http://booksshare.net/index.php?id1=4&category=cryptography&author=alferov-ap&book=2002.

Abbasov A.E., Abbasov T.E., 2015. Otsenka kachestva programmnogo obespecheniya dlya sovremennykh sistem obrabotki informatsii [Evaluation of software quality for modern information processing systems]. Informatsionno- tekhnologicheskiy vestnik [Information Technology Bulletin], 2015. Vol. 5. № 3. Pp. 15–27. https://www.elibrary.ru/item.asp?id=25360733.

Alekseychuk A.N., 2005. Sovershennye skhemy razdeleniya sekreta i konechnye universalnye algebry [Perfect secret separation schemes and finite universal algebras]. Analiz i obrabotka dannykh [Data Analysis and Processing], 2005. http://dspace.nbuv.gov.ua/bitstream/handle/123456789/50768/08-Alekseichuk.pdf?sequence=1

Bozkurt I.N., Selcuk G., 2008. Threshold cryptography based on blakely secret sharing. Information Sciences, 2008. Pp. 1–4. https://scholar.google.com/citations?user=0uolARoAAAAJ&hl=ru

Blakley G.R. et al., 1979. Safeguarding cryptographic keys. Proceedings of the national computer conference, 1979. Vol. 48. Pp. 313–317. https://ieeexplore.ieee.org/document/8817296.

Chervyakov N.I., Deryabin M.A., 2016. Novyy metod porogovogo razdeleniya sekreta, osnovannyy na sisteme ostat- ochnykh klassov [New method of threshold secret separation, based on the system of residual classes]. Informatsionnye tekhnologii [Information Technologies], 2016. Vol. 22. № 3. Pp. 211–219. http://novtex.ru/IT/it2016/it316_web-211–219.pdf .

Dingyi P., Arto S., Cunsheng D., 1996. Chinese remainder theorem: applications in computing, coding, cryptography. World Scientific, 1996. https://books.google.com/books/about/Chinese_Remainder_Theorem_Applications_I.html?id=RQLtCgAAQBAJ

Ito M., Saito A., Nishizeki T., 1989. Secret sharing scheme realizing general access structure. Electronics and Com- munications in Japan (Part III: Fundamental Electronic Science), 1989. Vol. 72. № 9. Pp. 56–64. https://archiv.infsec.ethz.ch/education/as09/secsem/papers/ItSaNi87.pdf

Karnin E., Greene J., Hellman M., 1983. On secret sharing systems. IEEE Transactions on Information Theory, 1983. Vol. 29, № 1. Pp. 35–41. https://ieeexplore.ieee.org/document/1056621

Kiparisova A.I., Azhmuhamedov I.M., 2016. Providing access to information systems of higher education in the case of loss of key information. Mezhdunarodnyy nauchno-issledovatelskiy zhurnal [International Research Journal], 2016. № 2–2 (44). https://cyberleninka.ru/article/n/providing-access-to-information-systems-of-higher-education-in-the-case-of-loss-of-key-information

Lavrinenko A.N., Chervyakov N.I., 2014. Nekotorye elementy kontseptsii aktivnoy bezopasnosti v sovremennoy kriptografii [Some elements of the concept of active security in modern cryptography]. Nauchnye vedomosti Belgorodskogo gosudarstvennogo universiteta. Seriya: Ekonomika. Informatika

[Scientific News of Belgorod State University. Series: Economy. Computer science], 2014. Vol. 30. № 8–1 (179). https://cyberleninka.ru/article/n/nekotorye-elementy-kontseptsii-aktivnoy-bezopasnosti-v-sovremennoy-kriptografii

Medvedev N.V., Titov S.S., 2011. Pochti porogovye skhemy razdeleniya sekreta na ellipticheskikh krivykh [Almost threshold secret separation schemes on elliptic curves]. Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki [Reports of Tomsk State University of Control Systems and Radioelectronics], 2011. № 1 (23). https://cyberleninka.ru/article/n/pochti-porogovye-shemy-razdeleniya-sekreta-na-ellipticheskih-krivyh

Moldovyan A.A. et al., 2011. Protokoly s nulevym razglasheniem sekreta i obosnovanie bezopasnosti skhem tsifrovoy podpisi [Protocols with zero disclosure of the secret and the justification of the security of digital signature schemes]. Voprosy zashhity informatsii [Information Security Issues], 2011. № 4. Pp. 6–11. https://www.elibrary.ru/item.asp?id=17100299

Mogilevskaya N.S., Kulbikayan R.V., Zhuravlev L.A., 2011. Porogovoe razdelenie faylov na osnove bitovykh masok: ideya i vozmozhnoe primenenie [Threshold file sharing based on bit-masks: idea and possible use]. Vestnik Donskogo gosu- darstvennogo tekhnicheskogo universiteta [Bullettin of the Don State Technical University], 2011. Vol. 11. № 10. https://www.vestnik-donstu.ru/jour/article/view/912

Petrov A., 2017. Kompyuternaya bezopasnost. Kriptograficheskie metody zashchity [Computer security. Cryptograph- ic methods of protection]. Moscow, Litres Publ., 2017. 114 p. https://www.iprbookshop.ru/87998.html

Piskova A.V., Korobeynikov A.G., 2015. Razrabotka algoritma elektronnoy tsifrovoy podpisi, osnovannogo na zadachakh faktorizatsii i diskretnogo logarifmirovaniya na ellipticheskikh krivykh [Development of an electronic digital sig- nature algorithm based on the problems of factorization and discrete logarithmization on elliptic curves]. Sbornik trudov IV Vserossiyskogo kongressa molodykh uchenykh [Proceedings of the IV All-Russian Congress of Young Scientists]. St. Peters- burg, ITMO University Publ., 2015. Pp. 322–326. https://kmu.itmo.ru/file/download/360

Parvatov N.G., 2008. Sovershennye skhemy razdeleniya sekreta [Perfect secret sharing schemes]. Prikladnaya dis- kretnaya matematika [Applied Discrete Mathematics], 2008, № 2 (2). Pp. 41–47. https://www.mathnet.ru/php/archive.phtml?wshow=paper&jrnid=pdm&paperid=33&option_lang=rus

Shenets N.N., 2011. Ob idealnykh modulyarnykh skhemakh razdeleniya sekreta v koltsakh mnogochlenov ot neskol- kikh peremennykh [On the ideal modular secret separation schemes in polynomial rings of several variables], 2011. http://elib.bsu.by/handle/123456789/9565

Shnayer B., Fergyuson N., 2005. Prakticheskaya kriptografiya [Practical cryptography]. Moscow, Dialektika, 2005. 480 p. https://www.labirint.ru/books/599557/

Sharyy S.P., 2012. Kurs vychislitelnykh metodov [The course of computational methods]. Novosibirsk, Novosibirsk State University Publ., 2012. http://www.ict.nsc.ru/matmod/files/textbooks/SharyNuMeth.pdf

Stadler M., 1996. Publicly verifiable secret sharing. International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1996. Pp. 190–199. https://crypto.ethz.ch/publications/files/Stadle96.pdf

VashchenkoG.V.,2009.VychislitelnayamatematikaOsnovyalgebraicheskoyitrigonometricheskoy interpolyatsii [Computational Mathematics. Basics of algebraic and trigonometric interpolation]. Sovremennye problemy nauki i obra- zovaniya [Modern problems of Science and Education], 2009. № 1. Pp. 54–55. https://edu-lib.com/matematika-2/dlya-studentov/vashhenko-g-v-vyichislitelnaya-matematika-osnovyi-algebraicheskoy-i-trigonometricheskoy-interpolyatsii-onlayn

МАЗМҰНЫ

СОДЕРЖАНИЕ

CONTENTS

Publication Ethics and Publication Malpracticein the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethicalguidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any otherlanguage, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайтах:
www:nauka-nanrk.kz
http://physics-mathematics.kz/index.php/en/archive
ISSN2518-1726 (Online),
ISSN 1991-346X (Print)

Заместитель директор отдела издания научных журналов НАН РК *Р. Жәлиқызы*
Редакторы: *М.С. Ахметова, Д.С. Аленов*
Верстка на компьютере *Г.Д.Жадыранова*

Подписано в печать 12.06.2023.
Формат 60х881/8. Бумага офсетная. Печать –ризограф.
19,0 п.л. Тираж 300. Заказ 2.

Национальная академия наук РК
050010, Алматы, ул. Шевченко, 28, т. 272-13-19