ҒТАХР 81.93.29

10.51889/2959-5894.2025.91.3.019

Н.А. Капалова[1], А.Ж.Абишева[2*]

[1]ҚР ҒЖБМ ҒК Ақпараттық және есептеу технологиялары институты, Алматы қ., Қазақстан
[2]Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы қ., Қазақстан
[*]*e-mail: ak_maral@mail.ru*

КРИПТОГРАФИЯЛЫҚ КІЛТТЕРДІ БАСҚАРУДЫҢ ЖӘНЕ САНДЫҚ ҚОЛТАҢБАНЫ ҚОЛДАНУДЫҢ ЗАМАНУИ ТӘСІЛДЕРІ БОЙЫНША МӘСЕЛЕЛЕРІ

Аңдатпа

Мақалада кілттерді басқару мен сандық қолтаңбаның бар мәселелерін талдау нәтижелері берілген, сонымен қатар модификацияланған Шнорр схемасының алгоритмі әзірленіп, сипатталған. Криптографиялық жүйелерде кілттерді басқарудың және сандық қолтаңбаның дәстүрлі емес алгоритмдерін жасауда криптографиялық процедуралардың сенімділігі мен тиімділігін арттыруға позициялық емес полиномды санау жүйесін қолдану айтарлықтай мүмкіндік беретінін дәлелдей отырып PGP тәріздес жүйесін құру ұсынылған. Бұл жүйеде кілттердің өмірлік циклінің барлық кезеңдерінде кілт қауіпсіздігін қамтамасыз ететін, сенім рөлін барынша азайтатын, кілттерді басқару жұмысын автоматтандыратын шешім қажет. Осы мақсатта криптографиялық алгоритмдерді қолдану ғана емес, сонымен қатар шифрлау кілттерін тиімді басқару маңызды болып табылады. Теориялық маңыздылығы схеманың тұрақтылығын негіздеуде, ал практикалық маңыздылығы тиімді және масштабталатын криптографиялық жүйелерді құру үшін қолдану мүмкіндігінде жатыр, сондай ақ кванттық шабуылдарға қарсы қорғанысты күшейту мақсатында ұсынылған тәсілдің әлеуетін көрсетеді.

Түйін сөздер: криптография, криптографиялық кілттерді басқару, кілттерді генерациялау, позициялық емес полиномды санау жүйесі, PGP, сандық қолтаңба.

Н.А. Капалова[1], А.Ж.Абишева [2]
[1]Институт информационных и вычислительных технологий КН МНВО РК, г.Алматы, Казахстан
[2]Казахский национальный университет имени аль-Фараби, г.Алматы, Казахстан

К ВОПРОСУ О СОВРЕМЕННЫХ ПОДХОДАХ УПРАВЛЕНИЯ КРИПТОГРАФИЧЕСКИМИ КЛЮЧАМИ И ПРИМЕНЕНИИ ЦИФРОВОЙ ПОДПИСИ

Аннотация

В статье представлены результаты анализа существующих проблем в управлении ключами и цифровой подписи, а также разработан и описан алгоритм модифицированной схемы Шнорра. Предлагается создать PGP подобную систему, доказывающую, что использование непозиционной полиномиальной системы счисления открывает значительные возможности для повышения надёжности и эффективности криптографических процедур при разработке нетрадиционных алгоритмов управления сертификатами ключей и цифровой подписи в криптографических системах. Эта система требует решения, которое обеспечивает безопасность ключей на всех этапах жизненного цикла ключей, минимизирует роль доверия и автоматизирует управление ключами. Для этого важно не только использовать криптографические алгоритмы, но и эффективно управлять ключами шифрования. Теоретическая значимость состоит в том, что показана надежность предлагаемой схемы, а практическая – в возможности использовать ее для создания эффективных и легко расширяемых криптографических систем, показывая, что предложенный подход может хорошо защищать данные от возможных квантовых атак.

Ключевые слова: криптография, управление криптографическими ключами, генерация ключей, непозиционные полиномиальные системы счисления, PGP, цифровая подпись.

N.A. Kapalova[1], A.Zh. Abisheva[2]
[1]Institute of Information and Computational Technologies CS MSHE RK, Almaty, Kazakhstan
[2]Al-Farabi Kazakh National University, Almaty, Kazakhstan

ON THE ISSUE OF MODERN APPROACHES TO CRYPTOGRAPHIC KEY MANAGEMENT AND APPLICATION OF DIGITAL SIGNATURE

Abstract

The article presents the results of the analysis of existing problems in key management and digital signature, and also develops and describes the algorithm of the modified Schnorr scheme. It is proposed to create a PGP-like system, proving that the use of a non-positional polynomial number system opens up significant opportunities for increasing the reliability and efficiency of cryptographic procedures in the development of non-traditional algorithms for managing key certificates and digital signatures in cryptographic systems. This system requires a solution that ensures key security at all stages of the key life cycle, minimizes the role of trust, and automates key management. To achieve this, it is important not only to use cryptographic algorithms, but also to effectively manage encryption keys. The theoretical significance is that the reliability of the proposed scheme is shown, and the practical significance is in the possibility of using it to create effective and easily expandable cryptographic systems, showing that the proposed approach can well protect data from possible quantum attacks.

Keywords: cryptography, cryptographic key management, key generation, non-positional polynomial number systems, PGP, digital signature.

Кіріспе

Ақпараттық қауіпсіздікті қамтамасыз ету – ақпараттық технологияларды дамытудың басым бағыттарының бірі. Осы салада шешілген мәселелердің ауқымы сандық және сапалық тұрғыда үнемі кеңеюде. Компьютерлік жүйелерде ақпаратты қорғау үшін қолданылатын негізгі құралдардың бірі криптографиялық түрлендірулер болып табылады. Заманауи криптографияның төрт басты бөлімі бар: симметриялы криптожүйелер, ашық кілтті жүйелері, электронды қолтаңба жүйесі, кілттерді басқару. Қазіргі уақытта криптожүйелер кілттерді пайдалануға негізделген. Әдетте, кілттерді басқару криптографиялық қосымшалардың ең осал тұсы болып табылады. Криптографиялық технологияны пайдалану қарапайым, бірақ кілттерді сақтау, кілттерді пайдалану және олардың өзара алмасуын қамтамасыз ету әлдеқайда қиын. Сенімділігі төмен кілттік сертификаттарды басқару жүйесі өте жақсы ұйымдастырылған жүйелердің сапасын төмендетеді, өйткені алгоритмнің бар қауіпсіздігі кілтке шоғырланған. Криптографиялық кілттерді жасау, оларды жинақтау және тарату, сақтау, жою міндеттері кілттерді басқаруға жатады. Кілттік сертификаттарды басқару ақпарат алмасудың құпиялығын, деректердің сәйкестілігін және тұтастығын қамтамасыз ету үшін шешуші рөл атқарады [1-4]. Криптографияның негізгі қағидаларының бірі криптографиялық ақпаратты қорғау жүйесінің тұрақтылығы толығымен оларда қолданылатын кілттердің қауіпсіздігі туралы болжамдарға негізделеді. Криптографиялық кілттерді басқаруға қатысушылардың іс-әрекеттерін үйлестіру жолдары, ашық кілтті инфрақұрылымда әрбір пайдаланушыға ашық кілт пен оның иесі арасында айқын және сенімді сәйкестікті орнатуға мүмкіндік беретін рәсім ашық кілтті сертификаттау механизмі қажет. Криптографиялық жүйелерде кілттерді басқару - деректер қауіпсіздігі, ақпараттың тұтастығы мен құпиялығы маңызды болып табылатын қазіргі әлемде сұранысқа ие болатын зерттеулер мен тәжірибенің негізгі саласы болып қала береді. Криптожүйелердің табысты жұмыс атқаруы үшін кілттерді генерациялау, шифрлау, дешифрлау, хабарламаға қол қою, қол таңбаны тексеру сияқты негізгі алгоритмдер дұрыс және тиімді орындалуы керек. Қолданылатын кілттік сертификаттарды басқару әдістері ашық кілттің құжатқа қол қойған тарапқа тиесілі екендігіне кепілдік беруі, сондай-ақ осы тараптың тиісті жабық кілттің иелігінде екендігіне кепілдік беруі керек. Кілттерді тарату және сақтау кезінде жабық және ашық кілттердің тұтастығы, сондай-ақ жабық кілттің құпиялылығы қадағалануы маңызды.

Зерттеу әдіснамасы

Көптеген шетелдік зерттеулер криптографиялық жүйенің қауіпсіздігі мен тиімділігін арттыру мақсатында кілттік сертификаттардың өмірлік циклін басқарудағы сертификаттарды шығару, тіркеу, жаңарту, жинақтау, архивтеу, пайдаланудан шығару және жою сияқты процесстерін автоматтандыруға ерекше назар аударады. Әртүрлі куәландыру орталықтары арасындағы сенім қатынастарын басқару әдістерін, сертификаттың иерархиялық және желілік құрылымдарын, сенім үлгілерін, құпиялығы бұзылған немесе мерзімі өтіп кеткен сертификаттарды, соның ішінде сертификаттарды қайтарып алу тізімдерін CRL және OCSP хаттамаларын пайдалану қарастырылады.

Келтірілген өмірлік циклдің жалпы сатыларында кілттің өмір сүру циклінің әртүрлі күйлерін немесе фазаларын, сондай-ақ олардың арасында ауысу шарттарын неғұрлым нақты анықтауға болады. Кілттік сертификаттардың өмірлік цикл кезеңдерінің негізгі күйлері төмендегідей:

- пайдаланушыны тіркеу;
- пайдаланушыны инициализациялау;
- кілтті жинақтау;
- кілтті орнату;
- кілтті тіркеу;
- кілтті штатты қолдану;
- кілтті алдын ала тағайындау;
- кілтті жаңарту;
- кілтті архивтеу.
- кілтті пайдаланудан шығару және жою.

Сертификат - бұл абоненттің идентификаторынан, оның ашық кілтінен және куәлікті беру уақыты мен оның жарамдылық мерзімі сияқты қосымша ақпарат, сенімді түрде өкілетті ұйым немесе сенімді адам қолымен жасалған деректер жиынтығы. Ол оны сақтау немесе жөнелту кезінде ашық кілтті алмастыру мүмкіндігін болдырмау үшін арналған. Сертификатты алған және электрондық сандық қолтаңбаны растағаннан кейін, ашық кілттің абонентке шынымен тиесілі екеніне көз жеткізуге болады.

Ашық кілтті алмастыру кезіндегі орын алатын сипатталған қаупі ашық кілт сертификаттарын пайдалану арқылы сәтті түрде жойылады. Ашық кілт сертификаттары ашық кілттер криптографиясында маңызды рөл атқарады және оның негізгі мақсаты - пайдаланушының ашық кілтін қол жетімді ету және жарамды ету. Оларды қалыптастыру X.509 стандартында ұсынылған қатаң аутентификация қағидаларына және ашық кілттердің криптожүйелерінің қасиеттеріне негізделеді. Ашық кілтті криптожүйелерде пайдаланушыда (барлығына қолжетімді) ашық және жабық кілттер бар деп есептейді. Әрбір пайдаланушы өзінің жабық кілтімен анықталады. Қос кілттің көмегімен кез-келген басқа пайдаланушы өзінің коммуникациялық серіктесі жабық кілттің нақты иесі екендігін анықтай алады [5].

Біздің елге келетін болса, Қазақстан үкіметі ұлттық қауіпсіздік сертификатын, оның ішінде оны қолдану ережелерін енгізуге арналған бірқатар заңнамалық актілерді бекітті («Қауіпсіздік сертификатын беру және қолдану ережесін бекіту туралы» Қазақстан Республикасы Ұлттық қауіпсіздік комитеті Төрағасының 2018 жылғы 27 наурыздағы № 23/н бұйрығы).

Бекітілген қауіпсіздік сертификатын беру ережесінде сертификат үш жыл мерзімге байланыс операторының өтініші бойынша берілетіндігі айтылған. «Байланыс туралы» жаңа заңға сәйкес операторлар қауіпсіздік сертификатын пайдаланып, трафикті шифрланған хаттамалар арқылы өткізуі керек. Телекоммуникация операторлары абоненттерге Интернетке қол жетімділіктің өзгеретін шарттары туралы хабарлау және абоненттер мен қосалқы операторлар арасында сертификатты тарату үшін жауап береді. Сертификатты қолдану ережелері байланыс операторынан оны пайдаланудың ұйымдастырушылық және техникалық жағдайларының құпиялығын қамтамасыз етуді талап етеді [6]. Ашық кілтті криптография концепциясының пайда болуын американдық ғалымдар У.Диффи мен М.Хеллманның

революциялық мақаласы жарияланған 1976 жылдан бастауға болады [7]. 1984 жылы Т.Эль-Гамаль [8] шифрлау үшін де, аутентификация үшін де қолдануға болатын Диффи-Хеллман жүйесінің жетілдірілген нұсқасын көпшілік назарына ұсынды. Криптожүйе жай сандағы дискретті логарифмді табу мәселесіне негізделген шекті өріс. Сондай-ақ жоғарыда сипатталған екі схеманың модификациясы болып табылатын К.Шноррдың [9] схемасы назар аударуға тұрарлық. Дискретті логарифмдеу қиындығына негізделген жүйелердің бірі болып табылады. Бұл схемалардағы негізгі ұғым қарабайыр түбір ұғымы.

Анықтама. Модуль бойынша алғашқы түбір – бұл бүтін сан n келесі шартты қанағаттандырады $g^{\varphi(n)} \equiv 1 \, mod \, n$ және $g^L \neq 1 \, mod \, n$ мұндағы $1 < L < \varphi(n)$.

Ашық кілттер криптография саласы үнемі қарқындап өсіп келе жатқан мәселелерді шешу үшін дамып келеді. Салыстыра кетсек, бұл аутентификацияның ең қауіпсіз әдісі болып табылады және ассимметриялық криптографиялық алгоритмдер кванттық есептеу құрылғысында жасалған шабуылдарға қарсы тұра алады. Бұл пайдаланушы үшін қолданыста іске асыру аясында қарапайымдылығына байланысты, яғни қарапайым құпиясөздер дүниежүзілік желіде аутентификацияның ең кең тараған әдісі болып табылады және барлық жерде қолданылады.

Постквантты криптография қазіргі уақытта келесі негізгі класстарды қамтиды:

- торлар теориясы;
- көп өлшемді квадраттық жүйелер;
- хэш функцияларға негізделген электрондық қолтаңбалар;
- алгебралық кодтау теориясы;
- эллиптикалық қисықтардың изогенездері;
- өру теориясы.

Осының ішінде хэш функцияға негізделген криптографияға хэш-функциялар арқылы құрастырылған электрондық қолтаңбалар кіреді, бұл олардың кванттық есептеу құрылғысына төзімділігін қамтамасыз етеді. Бұл тәсіл бір кілтте қолтаңбалардың шектеулі санын ғана жасай алады. Жүйенің тағы бір кемшілігі - қол қоюшы қол қойған хабарламалардың нақты санын жазуы керек [10]. Бұл жазбадағы қате жүйенің осалдығына әкеледі. Классикалық мысал ретінде 1979 жылы ұсынылған Р.Мерклдің қолтаңбасын алуға болады [11].

Қарастырып отырған Шнорр схемасының теориялық маңызды сипаттамасы хэш функциясының рандомизация параметрі r генерациясынан кейін бірден есептелетіндігі болып табылады. Бұл мүмкіндік қолтаңбаны қолдан жасаудың тиімді алгоритмдері бар болса, дискретті логарифм мәселесін шешудің де алгоритмдері бар екенін ресми түрде дәлелдеуге мүмкіндік береді [12]. Демек, бұл схеманың беріктігі туралы теориялық қағидаға келіседі, қауіпсіздікті бұзу қиындығы криптожүйе негізінде жатқан күрделі дискретті логарифм мәселесін шешуден қарапайым емес екенін көрсетеді.

Шнорр схемасы криптографиялық алгоритм болып табылады, ол кілттік сертификаттарды басқаруда, әсіресе сандық қолтаңбаны жасау үшін қолданылады. Ол нөлдік біліммен дәлелдеу (Zero Knowledge Proof) идеясына негізделген, бұл пайдаланушыға ақпараттың өзін ашпай-ақ кейбір ақпаратқа меншік құқығын дәлелдеуге мүмкіндік береді.

Шнорpp схемасының қысқаша классикалық мазмұны келтірілген:

Кілттерді генерациялау

p, q – жай сандар, мұндағы $q/(p-1)$; g группаның тудырушы элементі Z_p^*; k – кездейсоқ сан, $1 < k < q$; $y = g^k mod \, p$ – ашық кілтті жасау. Ашық кілт (p, q, g, y), Жабық кілт k.

М хабарламасы үшін қолтаңба есептеу келесі қадамдардан тұрады:

1. Бір реттік құпия кілт болып саналатын кездейсоқ сан генерацияланады $r, \; 1 < r < q$.
2. Есептеледі $R = g^r mod \, p$.
3. M хабарламасына R мәні қосылады $H: E = H(M||R)$ H хэш-функция мәні есептеледі. E мәні қолтаңбаның бірінші бөлігі болып табылады.
4. Қолтаңбаның екінші бөлігі есептеледі: $S = r + kE \; mod \; q$, мұндағы k– құпия кілт.

Қолтаңбаны тексеру.

1. R' есептеу: $R' = g^S y^{-E} \, mod \, p$.
2. $M||R'$ хэш мән есептеледі H: $E' = H(M||R')$.
3. E және E' мәндері салыстырылады. Егер $E = E'$, онда қолтаңба дұрыс болып саналады.

Зерттеу нәтижелері

Алгоритмнің ұтымды жақтарын ескере отырып, ЭСҚ үшін позициялық емес санау жүйесін қолдану арқылы өзгерту ұсынылды. Бұл жұмыста позициялық емес полиномды санау жүйелері (ПЕПСЖ) негізінде модификацияланған Шнорр алгоритмінің кезеңдерін сипаттадық. Құрылған алгоритм көмегімен кілттерді генерациялау, қолтаңбаны құру, қолтаңбаны тексеруді, кілттің өмірлік циклін тиімді ұйымдастыра отырып PGP тәріздес жүйе құру жұмысын атқарамыз. Осы жүйе арқылы хабарламалармен қауіпсіз алмасу жұмысын атқаруды ұсыну көзделіп отыр. Осылайша кілттік сертификаттарды сенімді басқару жүйесі қалыптасады. Сенімді басқару жүйесі кілттік сертификаттың көмегімен криптографиялық функцияларды орындауды іске асырады. Бұл функциялар сандық қолтаңбаны қалыптастыруды, сандық қолтаңбаны тексеруді, деректерді шифрлауды, деректердің шифрын шешуді, кілттерді шифрлауды, кілттерді шешуді, деректердің кездейсоқ және әдейі өзгерістерін анықтау үшін пайдаланылатын хабарламаның аутентификация кодтарын жасауды және тексеруді қамтуы мүмкін.

Кілттерді генерациялау

Позициялық емес полиномды санау жүйесін (ПЕПСЖ) құру жүргізіледі. ПЕПСЖ жұмыс негіздері ретінде келтірілмейтін екілік полиномдар $p_1(x), p_2(x), \dots, p_n(x)$ дәрежелері $a_1, a_2, \dots, a_n$ болатындай сәйкесінше, жұмыс негіздерінің дәрежелер қосындысы кілттің ұзындығымен тең болуы тиіс, яғни $\sum_{i=1}^{n} a_i = L$. Қалдықтар туралы Қытай теоремасын қанағаттандыратындай барлық жұмыс негіздері әртүрлі болуы қажет.

Бұл жүйеде кез келген $F(x)$ көпмүшелігі, дәрежесі a-дан кіші болса, $p_1(x), p_2(x), \dots, p_n(x)$ жұмыс негіздері бойынша, оның бөлінуінен қалған қалдықтар тізбегі, позициялық емес және жалғыз болып табылады.

Жай сандар $q_1, q_2, \dots, q_n$ – таңдаймыз, осы шартты қанағаттандыратындай $2^{a_i} - 1 = 0(mod \; q_i), \; i = \overline{1,n}$ (1<q_i < deg ($p(x)$)-1) және $p_i(x)$ әрбір жұмыс негіздері үшін примитивті элемент (көпмүшелік) $g_i(x)$ таңдалады, $0 < g_1(x), g_2(x), \dots, g_n(x) < P(x)$, осы шарттарды қанағаттанидартындай $g_i(x)^{deg(p_i(x))-1} = 1 \, mod \, p_i(x), \; i = \overline{1,n}$.

Кездейсоқ сандарды таңдаймыз $k_i < q_i, \; i = \overline{1,n}$ шартын қанақаттандыратындай. Бұл мәндер k_i құпия сақталуы қажет, өйткені ол жабық кілт ЖК = $\{k_i\}$ болып табылады.

Әрбір жұмыс негіздері үшін есептеледі $y_i(x) = g_i(x)^{k_i} mod \; p_i(x), \; i = \overline{1,n}$.

Ашық кілт АК = $\{P, Q, G, Y\}$, яғни $P = \{p_1(x), p_2(x), \dots, p_n(x)\}$, $Q = \{q_1, q_2, \dots, q_n\}$, $G = \{g_1(x), g_2(x), \dots, g_n(x)\}$, $Y = \{y_1(x), y_2(x), \dots, y_n(x)\}$.

Қолтаңба

A: Қолтаңба үшін $r_i < q_i$ кездейсоқ сандар таңдайды, $R_i = g_i(x)^{r_i} mod \; p_i(x), \; i = \overline{1,n}$

$A \to B$: қолтаңбаның бірінші бөлігін есептейді $E_i = H(M||R_i), \; i = \overline{1,n}$

A: қолтаңбаның екінші бөлігін есептейді $S_i = r_i + k_i * E_i mod \; q_i, \; i = \overline{1,n}$

$A \to B$: M хабарлама қолтаңбамен (E_i, S_i) жіберіледі.

Қолтаңбаны тексеру

B: есептейді $R_i' = g_i(x)^{S_i} y_i(x)^{E_i^{-1}} mod \; p_i(x)$,

$H(M||R_i) = E_i'$ хэш-мән есептеледі.

E_i және E_i' салыстырылады. Егер $E_i = E_i'$ тең болса, онда қолтаңба дұрыс болып табылады.

Бұл модификацияланған алгоритмнің құрылымы, оның қауіпсіз кілт алмасу үшін қажетті криптографиялық параметрлерді құруға арналғанын болжайды. Қарастырылып отырған схема пайдаланушылар арасында сенім принципі бойынша екі тараптың ашық кілттерінің

түпнұсқалығын растауға, PGP тәріздес құрылатын жүйедегі хаттамаларды түсіну және жүйе қауіпсіздігін сақтау үшін өте маңызды.

Дискуссия

Электрондық сандық қолтаңба схемасының немесе шифрлау схемасының криптотұрақтылығы әдетте битпен есептеледі, яғни ол сәтті шабуылдың есептеу күрделілігінің көрсеткіші ретінде түсініледі. Белгілі L биттік қауіпсіздік үшін схеманы бұзу үшін шабылдаушы орындауы қажет операциялар саны $M = 2^L$ болуы керек. Қажетті операциялардың саны операцияларына көбейсе немесе кемісе, онда қарсылық деңгейі $dM = \log_2 x$ мәніне артады немесе төмендейді. Кез келген ассиметриялық алгоритмнің қауіпсіздігі алгоритмнің өзінің құпиялылығына емес, кейбір бір жақты функцияны есептеудің күрделілігіне негізделген. Бұл қасиет криптожүйенің барлық компоненттеріне, шифрлау процесстеріне және сандық қолтаңбаларға қатысты.

Әлемдік криптографиялық ғылыми қауымдастық постквантық алгоритмдерге толық көшу алдында шешуі керек бірнеше маңызды аспектілер бар:

- постквантық алгоритмдерді орындау тиімділігін арттыру қажеттілігі;
- дәлелденген қауіпсіз постквантық хаттамаларды құру қажеттілігі;
- криптожүйелердің таңдалған параметрлеріне қойылатын талаптарды әзірлеу және олардың есептеу күрделілігін бағалау;
- постквантық алгоритмдердің қолайлылығын жақсарту қажеттілігі.

Бұл мәселелерді шешу үшін классикалық асимметриялық тәсілмен бірге постквантық тәсілді қолдануды ұсыну қисынды және уақтылы болып көрінеді

Постквантық стандарттарға көшу киберқауіпсіздік саласындағы соңғы онжылдықтардағы ең ауқымды реформалардың бірі болмақ. Оның жетістігі кванттық есептеулер теориялық саладан практикалық пайдалануға ауысатын дәуірде деректердің қауіпсіздігін қамтамасыз етуге көмектеседі [13].

Осыған байланысты мақалада криптографиялық жүйелердегі криптографиялық кілттік сертификаттарды басқаруда ПЕПСЖ қолданатын сандық қолтаңба алгоритмін зерттеу және талдау өзекті болып табылады.

ПЕПСЖ пайдалану кілттердің ұзындығын қысқартуға, сондай-ақ позициялық емес криптографиялық алгоритмдердің күші мен тиімділігін арттыруға көмектеседі. Тиімділікке осы жүйенің модульдік негіздерінде барлық арифметикалық операцияларды параллель орындауға мүмкіндік беретін ПЕПСЖ мүмкіндіктерінің арқасында қол жеткізіледі.

Сақталатын және жіберілетін ақпаратты криптографиялық қорғаудың дәстүрлі емес алгоритмдерін құруда ПЕПСЖ қолдану олардың тиімділігі мен криптографиялық төзімділігін айтарлықтай арттыруға мүмкіндік береді.

Аталған алгоритмдер шеңберінде белгіленген ұзындықтағы хабарламалар үшін электрондық сандық қолтаңбаны қалыптастыру процесі жүзеге асырылады. Позициялық емес криптографиялық жүйелерде криптографиялық беріктік кілттердің ұзындығымен ғана емес, сонымен қатар толық құпия кілтпен байланысты ЭСҚ алгоритмінің өзінің сипаттамаларымен де анықталады. Сонымен қатар, екілік коэффициенттері бар келтірілмейтін көпмүшеліктердің реттілігінің жоғарылауымен олардың айтарлықтай өсуі байқалады, бұл көпмүшелік негіздерін таңдаудың көптеген нұсқаларын береді.

Қорытынды

Қазіргі уақытта киберқауіптің өсуі, деректер құпиялығы мен тұтастығының бұзылуының жылдам қарқындауы, заманауи шабуылдардың күрделігі сияқты факторлар криптографиялық жүйелерде кілттерді басқарудың өзектілігін айқындайды. Internet of Things (IoT) және бұлтты есептеулер сияқты жаңа технологиялардың пайда болуы, оған сәйкесінше ақпарат алмасып отыратын қолданушылар саны және олардың қолданыстағы шифрлау алгоритмдері ұлғайып,

тасымалданатын деректер көлемі мен шифрлауды қажет ететін құралдар саны көбейген сайын кілттерді басқарудың күрделілігі күннен күнге артады. Осы орайда кілттік сертификатарды басқару мен криптография саласында қазіргі заманғы талаптарға бейімделген кілттерді басқарудың жаңа тәсілдерін құруды жоғары стандарттарға сай талап етеді және ақпараттық қауіпсіздіктің маңызды аспектісіне айналдырады.

Екілік көпмүшеліктердің дәрежесіне көбейтудің және дәрежелеудің барлық операциялары ПЕПСЖ жүйесінде орындалады, бұл осы операцияларды жүйенің негізі ретінде таңдалған $p_1(x), p_2(x), \dots, p_n(x)$ көпмүшеліктердің модульдері бойынша параллельді есептеуге мүмкіндік береді, нәтижесінде операция орындалу жылдамдығы артады.

Сонымен, ПЕПСЖ негізінде жасалған үш кезеңнен тұратын: 1) ПЕПСЖ жүйесін қалыптастыру; 2) электрондық сандық қолтаңбаны қалыптастыру; 3) электрондық сандық қолтаңбаны тексеру Шнорр асимметриялық шифрлау алгоритмінің модификациясы жүзеге асырылды.

Криптографиялық алгоритмдердің бағдарламалық жасақтамасы дәстүрлі аппараттық құралдармен бәсекелесе алады. Жұмыс негіздерді және оларға сәйкес примитивті көпмүшеліктерді, пайдаланушылардың жеке кілттерін таңдаумен ПЕПСЖ пайдалану, кілттік сертификаттарды басқаруда осы алгоритмнің криптографиялық күші ақпаратты қорғаудың сенімділігі мен тиімділігін арттырады. Кілттерді қауіпсіз сақтау, кілттерді пайдалану және кілттермен алмасу ұсынылып отырған криптографиялық ақпаратты қорғау жүйесінің маңызды бөлігі болып табылады. Кілттік сертификаттарды басқару жүйесі осылайша «сенім желісін» пайдалану негізінде кілттерді генерациялауға, сақтауға және таратуға, сондай-ақ шифрлау әдісін және позициялық емес полиномды санау жүйелеріне негізделген сандық қолтаңба алгоритмін пайдалануға арналған.

Кванттық технологиялардың пайда болу дәуірінде бұл схеманы, мысалы, тор теориясын пайдалана отырып, бейімдеуге болады. Мұндай жүйелерді дамытудың тағы бір маңызды бағыты кванттық шабуылдардың күрделілігін және қарапайым пайдаланушылар үшін шығындарды азайту қажеттілігін ескере отырып, интерфейсті жеңілдету және криптографиялық қорғауда процесстерді автоматтандыру тек мамандарға емес, сонымен қатар пайдаланушыларға қол жетімді болатындай, болашақта ақпаратты қорғайтын кванттық төзімді жүйелерді құрудың маңыздылығын атап өту маңызды.

Пайдаланылған дереккөздердің тізімі

[1] Barker E. (2016) Recommendation for Key Management – Part 1: General / NIST Special Publication 800-57, Revision 4. 160 p.

[2] Barker E., Smid M., Branstad D., Chokhani S. (2013) A Framework for Designing Cryptographic Key Management Systems / NIST Special Publication 800-130, Revision 4. 120 p.

[3] Капалова Н.А., Абишева А.Ж. (2019) Орталықтандырылған криптографиялық кілттерді басқару жүйесі // Матер. IV междунар. науч.-практ. конф. «Информатика и прикладная математика». – Алматы, 569-575.

[4] Варенников А.В. (2019) «Краткий обзор основных принципов разработки систем управления криптографическими ключами» // Матер. науч. конф. «Современные проблемы информатики и вычислительных технологий». – Алматы, 154-160.

[5] Капалова Н.А., Абишева А.Ж. (2020) Сандық сертификаттарды қолдану // Международная научно-практическая конференция "Актуальные проблемы информационной безопасности в Казахстане", Алматы, 46-54.

[6] Digital Report. (2016) Национальный сертификат безопасности Казахстана: Защита пользователей или государства? https://online.zakon.kz/Document/?doc_id=37226731#pos=4;-137

[7] Diffie W., Hellman M. E. (1976) New Directions in Cryptography, IEEE Trans. Inf. Theory / F. Kschischang - IEEE, Vol.22, Iss.6. - P.644-654. - ISSN 0018-9448 - doi:10.1109/TIT.1976.1055638

[8] Elgamal T. (1985) A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms // IEEE Trans. Inf. Theory / F. Kschischang - IEEE, - Vol. 31, Iss. 4. - P. 469–472. - ISSN 0018-9448 - doi:10.1109/TIT.1985.1057074.

[9] Schnorr C.P. (1990) Efficient Identification and Signatures for Smart Cards.Advances in Cryptology - CRYPTO'89. Lecture Notes in Computer Science 435. 239-252.

[10] Chen L., Jordan S., Liu Y.K., Moody D., Peralta R., Perlner R., Smith-tone D. (2016) Report on Post-Quantum Cryptography, NISTIR 8105, National Institute of Standards and Technology, Gaithersburg, https://doi.org/10.6028/NIST.IR.8105. Maryland, April, 10pp.

[11] Merkle, Ralph Charles. (1979) Secrecy, authentication, and public key systems : Technical Report No. 1979-1. - Citeseer, - doi:10.1.1.637.3952.

[12] D. Pointcheval, J. Stern. (2000) Security Arguments for Digital Signatures and Blind Signatures // Journal of Cryptology. V. 13. P.361-396.

[13] Darth Sahara. (2025) Великобритания опубликовала план перехода на криптографию, устойчивую к квантовым атакам, к 2035 году https://www.ixbt.com/news/2025/03/24/velikobritanija-opublikovala-plan-perehoda-na-kriptografiju-ustojchivuju-k-kvantovym-atakam-k-2035-godu.html

References

[1] Barker E. (2016) Recommendation for Key Management – Part 1: General / NIST Special Publication 800-57, Revision 4. 160 p.

[2] Barker E., Smid M., Branstad D., Chokhani S. (2013) A Framework for Designing Cryptographic Key Management Systems / NIST Special Publication 800-130, Revision 4. 120 p.

[3] Kapalova N.A., Abisheva A.Zh. (2019) Ortalyktandyrylgan kriptografijalyk kiltterdi baskaru zhyjesi [Centralized cryptographic key management system]. Mater. IV mezhdunar. nauch.-prakt. konf. «Informatika i prikladnaja matematika». Almaty, 569-575. (In Kazakh)

[4] Varennikov A.V. (2019) Kratkij obzor osnovnyh principov razrabotki sistem upravlenija kriptograficheskimi kljuchami. [A Brief Overview of the Basic Principles of Designing Cryptographic Key Management Systems]. Mater.nauch.konf. «Sovremennye problemy informatiki i vychislitel'nyh tehnologij». Almaty, 154-160. (In Russian)

[5] Kapalova N.A., Abisheva A.Zh. (2020) Sandyk sertifikattardy koldanu [Using digital certificates]. Mezhdunarodnaja nauchno-prakticheskaja konferencija "Aktual'nye problemy informacionnoj bezopasnosti v Kazahstane", Almaty, 46-54. (In Kazakh)

[6] Digital Report. (2016) Nacional'nyj sertifikat bezopasnosti Kazahstana: Zashhita pol'zovatelej ili gosudarstva? [National Security Certificate of Kazakhstan: Protecting Users or the State?] https://online.zakon.kz/Document/?doc_id=37226731#pos=4;-137 (In Russian)

[7] Diffie W., Hellman M. E. (1976) New Directions in Cryptography, IEEE Trans. Inf. Theory / F.Kschischang - IEEE, - Vol.22, Iss.6. - P.644-654. - ISSN 0018-9448 - doi:10.1109/TIT.1976.1055638

[8] Elgamal T. (1985) A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms // IEEE Trans. Inf. Theory / F. Kschischang - IEEE, - Vol. 31, Iss. 4. - P. 469–472. - ISSN 0018-9448 - doi:10.1109/TIT.1985.1057074.

[9] Schnorr C.P. (1990) Efficient Identification and Signatures for Smart Cards.Advances in Cryptology - CRYPTO'89. Lecture Notes in Computer Science 435. - C. 239-252.

[10] Chen L., Jordan S., Liu Y.K., Moody D., Peralta R., Perlner R., Smith-tone D. (2016) Report on Post-Quantum Cryptography, NISTIR 8105, National Institute of Standards and Technology, Gaithersburg, https://doi.org/10.6028/NIST.IR.8105. Maryland, April 2016, 10pp.

[11] Merkle, Ralph Charles. (1979) Secrecy, authentication, and public key systems : Technical Report No. 1979-1. - Citeseer. - doi:10.1.1.637.3952.

[12] D. Pointcheval, J. Stern. (2000) Security Arguments for Digital Signatures and Blind Signatures // Journal of Cryptology. V. 13. P.361-396.

[13] Darth Sahara. (2025) Velikobritanija opublikovala plan perehoda na kriptografiju, ustojchivuju k kvantovym atakam, k 2035 godu. [UK releases plan to move to quantum-resistant cryptography by 2035] https://www.ixbt.com/news/2025/03/24/velikobritanija-opublikovala-plan-perehoda-na-kriptografiju-ustojchivuju-k-kvantovym-atakam-k-2035-godu.html (In Russian)