ИНСТИТУТ ИНФОРМАЦИОННЫХ И ВЫЧИСЛИТЕЛЬНЫХ ТЕХНОЛОГИЙ КН МОН РК

30 YEARS OF INDEPENDENCE KAZAKHSTAN

VI - МЕЖДУНАРОДНАЯ НАУЧНО-ПРАКТИЧЕСКАЯ КОНФЕРЕНЦИЯ «ИНФОРМАТИКА И ПРИКЛАДНАЯ МАТЕМАТИКА»

МАТЕРИАЛЫ

29 сентября - 02 октября 2021 года

Институт информационных и вычислительных технологий МОН РК

МАТЕРИАЛЫ

VI международной научно-практической конференции "Информатика и прикладная математика" 29 сентября - 2 октября 2021, Алматы, Казахстан

Алматы 2021

УДК 378 (063)
ББК 74.58
И74

И 74 **Информатика и прикладная математика:** Мат. VI Межд. науч. конф. (29 сентября -2 октября 2021 г.). Алматы, 2021. – с. 490

ISBN 978-601-332-384-8

В сборнике опубликованы доклады, представленные от Республики Казахстан, Российской Федерации, США, Латвии, Польши, Республики Беларусь, Украины, Азербайджана, Узбекистана, Японии, Кореи, Ирана, Португалии, Испании, Великобритании, Греции, Кыргызской Республики и других.

Рассмотрены актуальные вопросы в области математики, информатики и управления: математического моделирования сложных систем и бизнес-процессов, исследования и разработки защищенных и интеллектуальных информационных и телекоммуникационных технологий, математической теории управления, технологий искусственного интеллекта.

Материалы сборника предназначены для научных работников, докторантов и магистрантов, а также студентов старших курсов.

УДК 378 (063)
ББК 74.58

ISBN 978-601-332-384-8

ХЕШТЕУ АЛГОРИТМДЕРІН ЖАСАУДАҒЫ БЛОКТЫ ШИФРЛАУ АЛГОРИТМДЕРІН ҚОЛДАНУ ЕРЕКШЕЛІКТЕРІ

С.Нысанбаева, Қ. Сақан
e-mail: sultasha1@mail.ru, kairat_sks@mail.ru
Ақпараттық және есептеуіш технологиялар институты ҚР БҒМ ҒК, Қазақстан

Аңдатпа. *Мақалада қазіргі ақпараттану кезеңіндегі мәліметтерді хештеудің маңыздылығы, ерекшеліктері және пайдалану аумағы жайлы айтылады. Хештеу алгоритмдерінің жасау процесінде симметриялық блоктық шифрлеу алгоритмін негізге алу, пайдалану мүмкіндіктері, құрылымдық қасиеттері, ерекшеліктері, сондай-ақ олардың осал және басым тұстары көрсетілген. Жұмыс нәтижесі арқылы шифрлау алгоритмнің пайдалануына қойылатын талаптер мен ұсыныстар баяндалған.*

Кіріспе

Қазіргі таңда сандық технологияның шарықтап даму кезеңіндегі заманауи қауіпсіз хэш алгоритмдері көптеген компьютерлік жүйелердегі ақпарат пен деректердің тұтастығы мен жарияланбауы үшін өте маңызды екендігі белгілі. Ақпараттық қауіпсіздіктің бұл талаптарын қамтамасыз ету мақсатында «хештеу» термині, осыған сәйкес хештеу алгоритмдері қолданылады, яғни ол ассоциативті массивтерді құру кезінде, деректер қорында көшірмелерді іздеу кезінде, деректер қоры үшін бірегей идентификаторларды құру кезінде, деректерді сақтау және/немесе беру кезінде туындайтын кездейсоқ немесе қасақана жасалынған өзгертулердің бар-жоғын, қауіпсіздік жүйелеріндегі парольдерді хеш ретінде сақтаған кезде, электрондық құжаттарға электрондық цифрлық қолтаңбаны жасау кезінде пайдаланылады.

Хештеу (hash - араластыру, араластыру, араластыру) – бұл кіріс хабарламалар массивін тұрақты ұзындықтағы мәліметке дейін түрлендіру (хеш, хеш-код немесе дайджест деп аталады). Хештің ерекшелігі – ұзындығы бастапқы берілген дерекке қарағанда едәуір қысқа болып келеді және бастапқы дерек пен оның хеші арасында жоғарғы ықтималдықпен екеуара өзара сәйкестіктің болуы. Өзара сәйкестікті қамтамасыз ету мақсатында қолданылатын математикалық түрлендіру хеш-функциялар (криптографиялық хеш-функциялар) көмегімен жүргізіледі. Уақыт өте келе ең кеңінен қолданылатын криптографиялық хеш функциялардың өздерінен айтарлықтай кемшіліктері анықталуда [1, 2].

Ақпаратты хештеу функцияларына қойылатын негізгі талаптарды айқындау

Жалпы жағдайда, бастапқы деректер мен оның хеші арасында өзара бірге-бір сәйкестік бола бермейді, яғни коллизиялардың (соқтығысулардың) бар болуы. Бірдей хеш беретін әртүрлі деректер жиынтығы бар болуы мүмкін, осындай сәйкестіктердің бар болуы ықтималдығын азайту – хеш-функцияға қойылатын негізгі талап болып саналады. Сондықтан, түпнұсқалықты қамтамасыз ету үшін хештеу алгоритмін қиындату немесе барынша жақсару заманауи хеш-алгортмдер жасауға негіз болып отыр. Осыған сәйкес жасалынатын криптографиялық хеш-функция төмендегідей негізгі сипаттамаларға ие болуы міндетті:

- кез-келген ұзындықтағы деректерді белгіленген ұзындықтағы хешке түрлендіру орындай алуы керек;
- үлкен есептеу ресурстарын қажет етпеуі керек және жылдам орындалуы керек;
- хеш-функцияның криптографиялық тұрақтылығын зерттеу үшін оның алгоритмі ашық болуы керек;
- хештеу процесі (түрлендіруі) бір жақты болуы керек, яғни хеш бойынша бастапқы деректерді анықтауға математикалық мүмкіндік болмауы керек;
- ол коллизияларға «қарсы» болуы керек, яғни әртүрлі деректерге сәйкес бірдей хеш табу есептеулер күрделілігі жағынан мүмкін болмау керек;
- деректердің шамалы өзгеруіне сәйкес хеш айтарлықтай өзгеруі керек (лавиндік эффект).

Бұдан әрі, осы сипаттамалар негізінде жасалған криптографиялық хэш функциясы криптоталдау шабуылдардың барлық белгілі түрлеріне төтеп бере алуы керек. Теориялық криптографияда хеш функциясының қауіпсіздік деңгейі келесі қасиеттерді қолдана отырып анықталады:

- соқтығысуға (коллизияға) төзімділік,
- алғашқы бейнеге қарсылық (прообразға төзімділік),
- екінші алғашқы бейнеге қарсылық (екінші прообразға төзімділік).

Хеш функциялары жұмысы істеу тәртібін қарастырғанда, M хабарламаны хештеудің ең ыңғайлы әдісі: алдымен оны бірнеше бірдей бөліктерге (блоктарға) бөліп, содан кейін осы бөліктерді итеративті және жүйелі түрде өңдеу екені белгілі. Бүгінгі таңда параллель процессорлардың көмегімен бұл итеративті түрде тізбектеп хеш алу хэш әдісі тіпті кеңінен қолданылады.

Жалпы жағдайда, кез-келген хеш-функция болмаса хештеу алгоритмі екі компоненттен тұрады: f сығу функциясы және H конструкциясы. Сығу функциясы – бұл бекітілмеген үлкен өлшемдегі кірісті бекітілген аз өлшемдегі шығысқа сәйкес келтіретін $f : \{1, 0\}^m \rightarrow \{1, 0\}^n$ функция, мұндағы $m > n$. Конструкция – бұл M хабарламасын $M_1, M_2, \ldots, M_t$ бөлліктерге бөліп, оларды өңдеу үшін f қысу функциясын бірнеше рет жұмыс жасату (шақыру) тәсілі.

Хештеу алгоритмдерін жасаудағы блокты шифрлау алгоритмдерін қолдану жолдары

Хештеу алгоритмдерінде f сығу функциясы ретінде қандай да бір симметриялы блоктық шифрлау алгоритмін қолдануға болады. Мысалы, Ресейде ГОСТ Р 34.11-94 хештеу стандарты ресейлік ГОСТ 28147—89 криптографиялық шифрлау стандарты негізінде жасалған. Ал, қазіргі ГОСТ Р 34.10-12 («Стрибог» хештеу алгоритмі) стандарты да XSPL шифры негізіндегі ГОСТ Р 34.11-2012 стандартындағы блок шифры алынды. Көбінесе, шифрлау алгоритмі жолымен хештеу алгоритмдерінде белгілі Меркл-Дамгард конструкциясы пайдаланады. Коллизияға төзімділікті жоғарлатып, хеш функция қауіпсіздігін қамтамасыз ету мақсатында Меркл-Дамгард конструкциясының жаңа модификациялары бар. Соның бірі – Стефан Лакс ұсынған wide-pipe конструкциясы [3]. Бұл әдіс ұзындықты ұзарту шабуылына (“length extension” attack) ұшыраған Меркл-Дамгардтағы кемшіліктерді жою үшін ұсынылды. wide-pipe конструкциясы хешті есептеу үшін екі f және g қысу функциясынан тұрады. Еркін ұзындықтағы хабарлама толтырылғаннан кейін f функциясы кезекті b-биттік хабарлама бөлігін итеративті өңдеу үшін және нәтижесінде w-биттік аралық хештер алу үшін қолданылады. Хабарлама толықтай өңдегеннен кейін, g функциясы w-биттік соңғы аралық хешті қабылдап, одан n

биттік ақырғы хешті алу үшін қолданады: $f: \{1, 0\}^w \times \{1, 0\}^b \rightarrow \{1, 0\}^w$, $g: \{1, 0\}^w \rightarrow \{1, 0\}^w$, мұнда $w \geq n$.

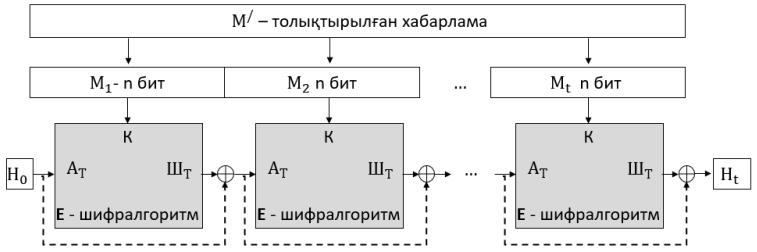
Қауіпсіздікті қамтамасыз ету үшін кілт ретінде берілген итерацияда хэштеуге арналған хабарламалар бөлігін, ал сығу функциясының алдыңғы шақырылымдағы нәтижесі кіріс ретінде, болмаса, кірістерін керісінше еті те алуға болады. Содан кейін соңғы итерацияның нәтижесі алгоритмнің шығысы, яғни ақырғы нәтижесі хеш болып есептелінеді [4]. Бұл жағдайда хеш фукциядағы сығу функциясы рөлін шифрлау алгоритмі орындайды. хеш функциясының қауіпсіздігі қолданылатын алгоритмнің қауіпсіздігіне негізделген. Осы процестің жалпы нұсқасын төмендегі сурет-1-ден көруге болады.

Сурет-1 – Блоктық шифрлау алгоритмі негізіндегі хеш функциясының жалпылама сұлбасы

Меркл-Дамгард конструкциясын негізге алып, ондағы f сығу функциясы ретінде E блоктық шифрын қолдану – аталған конструкцияның әрі қарай жетілдіруге келді [3]. Себебі, қолданылатын E блоктық шифрына біржақтылықты (односторонность) қамтамасыз ету керек. Біржақты функция – кез-келген кіріс мәні үшін оңай есептелетін математикалық функция, бірақ кері қарай, яғни, алынған мән арқылы функцияның аргументін табу қиын. Осыған сәйкес Пренель, Говертс және Вандевалль (Preneel, Govaerts and Vandewalle) $E: \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ блоктық шифры негізінде жасалатын f хеш-функцияның 64 түрлі әдісін қарастырды [5]. Кейде бұл осы 64 схеманың қауіпсіздігін зерттеу үшін шабуылдарға негізделген талдау әдістерін қарастырған осы авторлардың аты-жөндерімен байланыстырып, PGV схемалары деп атаған. Алдымен 12 PGV схеманың қауіпсіз екендігі, яғни коллизияларға төзімді екендігі дәлелденді, кейін тағы 8-і қосылды [6].

Бірқатар схемаларда аралық хеш мәні мәтін блогымен модуль 2 бойынша қосылу операциясы пайдаланылады. Бұл жағдайда шифрдағы кілт пен блоктың ұзындықтары бірдей болады. Шифрдегі кілт пен блоктың ұзындықтары сәйкес келген жағдайда тәжірибеде кең таралған ең қарапайым схема жайлы тоқталайық. Ескере кететіні, осы схемаларда бастапқы $H_0 = IV$ ретінде қарастырылады, мұндағы: IV – бастапқы вектор, ол көп жағдайларда нөлдік вектор деп алу енгізілген.

Дэвис-Мейер схемасы мына тәртіпте жұмыс істейді: $H_i = f(H_{i-1}, M_i) \oplus H_{i-1}$, $i = 1,2, \dots, t$, мұнда қысу функциясы ретінде E шифрлау алгоритмі, K кілт ретінде кезекті M_i хабарлама бөлігі, A_T ашық мәтін ретінде алдыңғы итерация мәні H_{i-1}, ал $Ш_T$ шығыс ретінде H_i аралық хеш мәні болады. Е шифрлау алгоритмі нәтижесі H_{i-1} – алдыңғы итерация мәнімен XOR операциясы арқылы біріктіріліп, соңында жаңа H_i – аралық хеш мәнді алатын боламыз. Бұл схема негізінен Рабин схемасын қайталайды, тек «Орта ақпарат» («Сведения в середину») шабуылынан қорғау үшін пайдаланады, схеманың графиктік бейнесі сурет-2 көрсетілген.



Сурет-2 - Дэвис-Мейер схемасы жұмыс тәртібі

Хештеу алгоритмдерін жасаудағы блокты шифрлау алгоритмдерін қолдану ерекшеліктері мен талаптары

f сығу функциясы негізін блоктық шифрлау алгоритмі ретінде қарастырғанда, хеш функцияның криптографиялық қауіпсіздігі қолданылатын шифрлау алгоритмнің қауіпсіздігіне негізделген болады [4]. Сондықтан, хештеу алгоритміндегі f сығу функциясы ретінде шифрлау алгоритмін пайдаланғанда, шифрлау алгоритмдерде төмендегідей талаптарды ескеру керек:

- күштік шабуылдарға криптографиялық беріктілік (аралық және қосымша нәтижелерді сақтау үшін және уақытша өлшем бойынша талап етілетін жадтың қажетті ең аз көлемі бойынша);
- ашық, жабық және шифрлау кілті (біздің жағдайда алдыңғы итерациядағы аралық хеш мән, кілт ретінде алынатын хабарлама бөлігі және осы итерациядан алынған аралық хеш мән, сәйкесінше) арасындағы өзара байланысты сипаттайтын алгебралық (логикалық) теңдеулер жүйесін табу және шешу тәсілдерінің болмауы;
- алгоритмге белгілі аналитикалық криптошабуылдарды іске асырудың практикалық қол жетімсіздігі немесе олардың жоғары есептеу күрделілігі;
- заманауи инновациялық-технологиялық дамудың қарқынын ескере отырып, алгоритмнің оңтайлы «криптографиялық беріктілік қорының» болуы;
- алгоритмнің жеңілдетілген нұсқасының криптографиялық беріктілігі, ондағы кейбір опцияның операцияларын қарапайым нұсқалармен алмастырыла алуы немесе жеңілдетіле алуы;
- шифрдың шығыс мәтінінің (аралық хеш мәнінің) статистикалық көрсеткіштері шынайы кездейсоқ тізбектің көрсеткіштеріне ұмтылуы тиіс.

Сонымен қатар, хеш алгоритмдері үшін пайдаланатын блоктық симметриялы алгоритмдерді жобалау мен талдау кезеңінде төмендегідей тәсілдерді ескеру ұсынылады [7]:

- «консервативті дизайн», яғни тек бірнеше рет тексерілген, яғни сенімді құрылымдарды, криптографиялық примитивтер мен кепілдендірілген қауіпсіздік әдістері пайдалану керек;
- барлық белгілі криптоталдаулық шабуылдарға беріктілік;
- алгоритмді жобалаудың қолжетімді және қарапайым құрылымы мен қағидаттары;
- алгоритмнің оңтайлы «төзімділік қорын» қалыптастыру, есептеу техникасы құралдарының ықтимал криптоталдаулық шабуылдарының пайда болуын ескеріп, алгоритмді одан әрі қауіпсіз пайдалану мүмкіндігі болуы;
- алгоритмнің барлық ықтимал осалдықтарынан қорғауды қамтамасыз ету;
- үздік әлемдік көрсеткіштерге жақын жоғары өнімділікті және беріктілікті қамтамасыз ету.

Қорытынды

Блоктық шифлау алгоритмдері негізінде хеш алгоритмдерін жасау барысында оған қойылатын алғышарттар, талаптар мен ұсыныстар нақтыланды. Соның негізінде алдағы уақытта біржақтылықты қамтамасыз ете алатын блоктық шифрлау алгоритмі жасалынып және Меркл-Дамгард конструкциясының wide-pipe модификациясын пайдаланып, параллельдік есептеуіштерде жұмыс істеуге мүмкіндік беретін хештеу конструкциясы құрылуда. Негізгі басымдық хеш функцияның негізгі үш қасиетіне ие болатын, сондай-ақ жұмыс өнімділігі бойынша заманауи әлемдік көрсеткіштерге сай хештеу алгоритмі жасалуда.

Алғыс

Ғылыми зерттеу жұмысы Ақпараттық және есептеуіш технологиялар институтында орындалып жатқан «Электрондық цифрлы қолтаңба үшін еркін ұзындықтағы хэштеу алгоритмін құру мен зерттеу және олардың беріктілігін бағалау» бағдарламалық-нысаналы қаржыландыру жобасы аясында орындалды.

Әдебиеттер

1. Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu, "Finding collisions in the full SHA-1," in Proceeding of CRYPTO'05, vol. 3621, 2005, pp. 17-36.
2. Marc Bevand, "MD5 Chosen-prefix collisions on GPUs," in Black Hat USA, Las Vegas, 2009.
3. Hirose, S. Some plausible constructions of double-blocklength hash functions. Fast Software Encryption, LNCS, Springer-Verlag, 2006, 4047, 210-225
4. Авезова Я.Э. Современные подходы к построению хеш-функций на примере финалистов конкурса SHA-3 // Вопросы кибербезопасности. 2015. №3 (11). URL: https://cyberleninka.ru/article/n/sovremennye-podhody-k-postroeniyu-hesh-funktsiy-na-primere-finalistov-konkursa-sha-3 (дата обращения: 10.08.2021).
5. Thomas Ristenpart and Thomas Shrimpton. How to build a hash function from any collision-resistant function. In Asiacrypt’07, vol. 4833, pp. 147-163. Springer-Verlag, 2007.
6. John Black, Phillip Rogaway, and Thomas Shrimpton. Black-box fnalysis of the block-cipher-based hash-function constructions from PGV. In Crypto’02, vol. 2442, pp. 320-335. Springer-Verlag, 2002.
7. Горбенко И.Д., Долгов И.В., Олейников Р.В., Руженцев В.И., Михайленко М.С., Горбенко Ю.И. Разработка требований и принцип проектирования перспективного симметричного блочного алгоритма шифрования // Известия ЮФУ. Технические науки. 2007. №1. URL: https://cyberleninka.ru/article/n/razrabotka-trebovaniy-i-printsip-proektirovaniya-perspektivnogo-simmetrichnogo-blochnogo-algoritma-shifrovaniya (3.11.2020).

МАТЕРИАЛЫ
VI международной научно-практической конференции
"Информатика и прикладная математика",

29 сентября - 2 октября 2021, Алматы, Казахстан

Подписано в печать 25.09.2021 г. Формат А4
Печать цифровая. Бумага офсетная. Усл. печ. л. 51.45.
Тираж 300 экз. Заказ № 006900.
Отпечатано в ИИВТ МОН РК.
Алматы, ул. Пушкина, 125