ХЕШ ФУНКЦИЯ АЛГОРИТМЛАРИ ВА УЛАРНИНГ ҚУРИЛИШ ТАМОЙИЛЛАРИ ТАҲЛИЛИ

Нодир Расулович ЗАЙНАЛОВ
доцент
Техника фанлари номзоди
Тошкент ахборот технологиялари университети Самарқанд филиали
Самарқанд, Ўзбекистон
nodirz@mail.ru
Ойбек Шакарбой ўғли УМУРЗАҚОВ
Ассистент
Тошкент ахборот технологиялари университети Самарқанд филиали
Самарқанд, Ўзбекистон
oybekumurzaqov1993@gmail.com

Аннотация

Мақолада хеш функция алгоритмларига қўйиладиган умумий талаблар, хеш функцияларнинг ахборот тизимларида қўлланилиши, хеш функцияларни қуриш схемалари, шифрлаш алгоритмлар асосида хеш функцияларни қуриш тамойиллари ва формулалари ҳақида таҳлиллар натижалари келтирилган.

Таянч сўзлар: хеш функция, хеш функциялар мақсади, хеш функцияларни қуриш тамойиллари.

АНАЛИЗ АЛГОРИТМОВ ХЕШ-ФУНКЦИЙ И ПРИНЦИПОВ ИХ ПОСТРОЕНИЯ

Нодир Расулович ЗАЙНАЛОВ
доцент
Кандидат технических наук
Самаркандский филиал Ташкентского университета информационных технологий
Самарканд, Узбекистан
nadirz@mail.ru
Ойбек Шакарбой угли УМУРЗАКОВ
Ассистент
Самаркандский филиал Ташкентского университета информационных технологий
Самарканд, Узбекистан
oybekumurzaqov1993@gmail.com

Аннотация

В статье представлены результаты анализа общих требований к алгоритмам хеш-функций, использования хеш-функций в информационных системах, схем построения хеш-функций, принципов и формул построения хеш-функций на основе алгоритмов шифрования.

Ключевые слова. хеш-функция, назначение хеш-функций, принципы построения хеш-функций.

Хеш функция деб ихтиёрий узунликдаги *M* маълумотни фиксирланган узунликдаги *H(M)* қийматга акслантирувчи функцияга айтилади. Бу ерда фиксирланган узунлик сифатида 64 бит, 128 бит, 160 бит, 256 бит, 512 бит тушунилади.

“Хеш” сўзи инглиз тилидаги «Hash» сўзидан олинган бўлиб, унинг маъноси “шовқин” ёки “аралаш” каби таърифланади. Аслида, булар атаманинг ҳақиқий маъносини тўлиқ ифодалайди [13].

Одатда “хешлаш” – бу жараён бўлиб, инглиз тилида – чопиш, аралаштириш каби маъноларни англатади.

Хешлаш – бу кириш маълумотлари массивини детерменистик алгоритм асосида чекли узунликдаги чиқиш сатрига айлантиришдир.

Бошқача айтганда, хешлаш – бу шундай жараёнки, унда кириш массивидаги маълумотлар махсус алгоритм асосида битлар кетма-кетлигига алмаштирилади.

Хеш функция алгоритмларидан амалий фойдаланишдан кўзланган асосий мақсад:

1. Маълумотни узатишда ва сақлашда унинг тўлалигини назорат қилиш.

2. Маълумот манбаъсини аутентификация қилиш.

Бугунги кунда хеш функция алгоритмларига қўйидагича умумий талаблар қўйилади.

1. Ихтиёрий узунликдаги матнга қўллаб бўлиши.

2. Чиқишда тайинланган қийматни бериши.

3. Ихтиёрий берилган *x* бўйича *H(x)* ни осон ҳисобланиши.

4. Ихтиёрий берилган *H* функция бўйича $H(x) = h$ тенгликдан x ни ҳисоблаб топиб бўлмаслиги (бир томонламалик хоссаси).

5. Олинган *x* ва y $(y \neq x)$ матнлар учун $H(x) \neq H(y)$ бўлиши (коллизияга бардошлилик хоссаси).

Умумий ҳолда хеш-функция алгоритмлари икки турга бўлинади [8]:

1. Калитли хеш функциялар.

2. Калитсиз хеш функциялар.

Калитли хеш функция – симметрик калитли тизимларда ишлатилади. Калитли хеш функциялар берилган маълумот аутентификацияси коди (message authentication code (MAC)) деб ҳам юритилади. Ушбу код бир-бирига ишончи мавжуд фойдаланувчиларга берилган маълумотнинг ҳақиқийлиги ва тўлалиги кафолатини қўшимча воситаларсиз таъминлаш имкониятини туғдиради [1].

Калитсиз хеш функциялар хатоларни топиш коди (modification detection code (MDC) ёки manipulation detection code, massage integrrity code (MIC) деб аталади. Ушбу код қўшимча воситалар (масалан, ҳимояланган алоқа тармоғи, шифрлаш ёки ЭРИ алгоритмлари) ёрдамида берилган маълумот тўлалигини кафолатлайди. Бу турдаги хеш функциялардан бир-бирига ишонч билдирувчи ва ишончи бўлмаган томонлар фойдаланишлари мумкин [10].

Хеш функциялар асосан, Электрон рақамли имзо (ERI)да, Torrent, DC Hub, Операцион системаларда ва файлларнинг бутунлилигини ёки ўзгартирилганлигини назорат қилиш учун фойдаланилади. Ахборот бутунлигини назорат қилишнинг кўпроқ мақбул бўлган методларидан бири хеш-функциядан фойдаланиш ҳисобланади. Хеш функциянинг қийматини унинг калитини билмасдан туриб қалбакилаштириб бўлмайди, шу сабабли хешлаш калитини шифрланган кўринишда хотирада сақлаш зарур.

Ушбу тизимларга кирадиган алгоритмлар 1-жадвалда келтирилган.

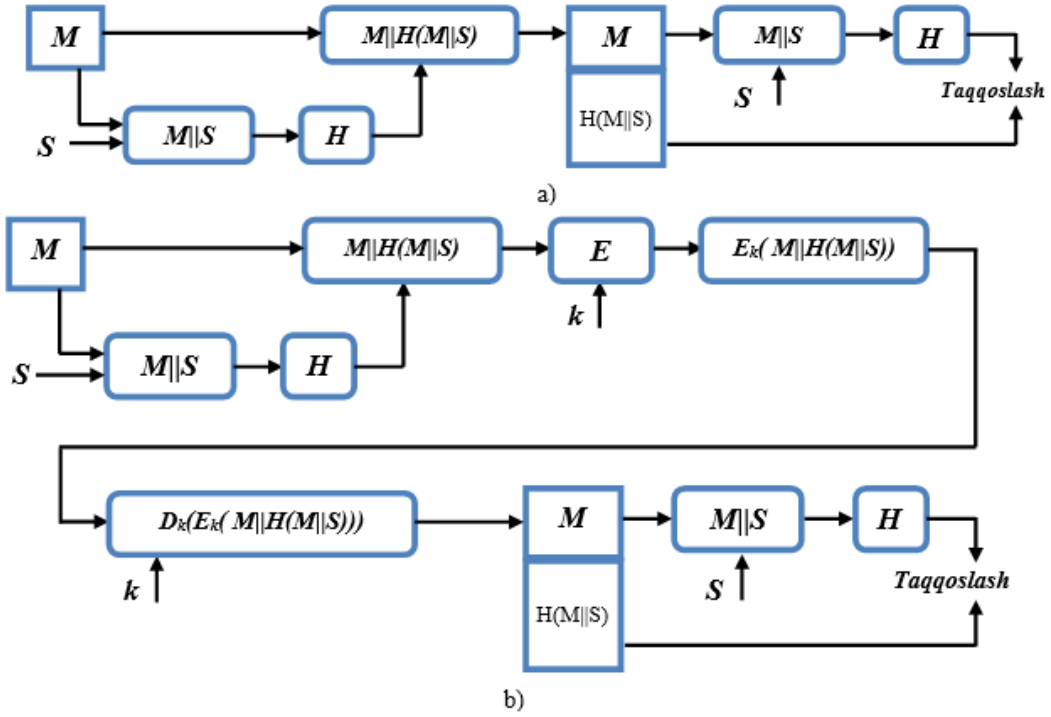
1-жадвал

Калитли ва калитсиз хеш функциялар

Калитсиз хеш-функциялар	Калитли хеш-функциялар
ГОСТ Р 34.11-94 MD SHA СТБ 1176.1 – 99 RIPE-MD TIGER HAVAL ... ва бошқ.	O‘z DSt 1106 : 2009 RIPE-MAC N-хэш MD5-MAC MAA CBC-MAC CRC-MAC ... ва бошқ.

Мазкур хеш алгоритмларлар ҳақида маълумотлар фойдаланилган адабиётлар ва интернет манбаларида келтирилган.

Умумий ҳолда хеш функцияларни ахборот-коммуникация тизимларида қўлланилиши 1-расмда келтирилган [9].



M – маълумот, H – хеш функция , S – назорат суммаси,
a) – маълумотни фақат хеш-функция ёрдамида хешлаш жараёни
b) – хешланган маълумотни узатишда шифрлаш алгоритмларидан фойдаланиш.

1-расм. Хеш функцияларни ахборот-коммуникация тизимларида қўллаш схемаси.

Хеш функция маълумот қисм блоклари устида кетма-кет акслантиришлар ва қадамба-қадам амалга оширилувчи (итератив) механизмлар ёрдамида ҳисобланади. Акслантиришлар ҳар бир блок устида бажарилиб, улар раунд акслантиришлари деб номланади ва хеш функцияда раунд функциялари кўринишида амалга оширилади. Акслантиришлар натижаси сифатида ушбу қадамда ҳисобланган хеш функциянинг раунд қиймати барча олдинги хеш функция қийматлари ва жорий блокдаги маълумот қийматига боғлиқ бўлади. Бу эса хеш функцияда илактириш механизмининг қўлланилишига олиб келади [14].

Умуман хеш функция раунд блокининг хеш қиймати H_i хеш функцияси F нинг иккита аргумент, яъни: олдинги раунддаги хеш функция

қиймати H_{i-1} ва жорий блокдаги маълумотнинг қиймати M_i га боғлиқ ҳолда ҳисобланади.

$$H_i = F(H_{i-1}, M_i), \quad i = 1,2, \ldots\ldots n, \qquad (1)$$

бу ерда H_0 - махсус ўзгармас(фиксирланган) бошланғич қиймат.

Хеш функциянинг блокли акслантиришларида F-функциянинг мураккаблигини ошириш мақсадида блокли шифрлаш ёки бир томонли функциялардан фойдаланиш мумкин. Бундан ташқари сиқувчи F функциялар, яъни: кириш блокига берилган маълумотнинг ўлчамини чиқиш блокида ундан кичик ўлчам(разряд)га акслантирувчи функциялардан фойдаланилади. Чиқувчи ҳар бир раунддаги H_i ўзгарувчи эса илактириш ўзгарувчиси деб номланади [5].

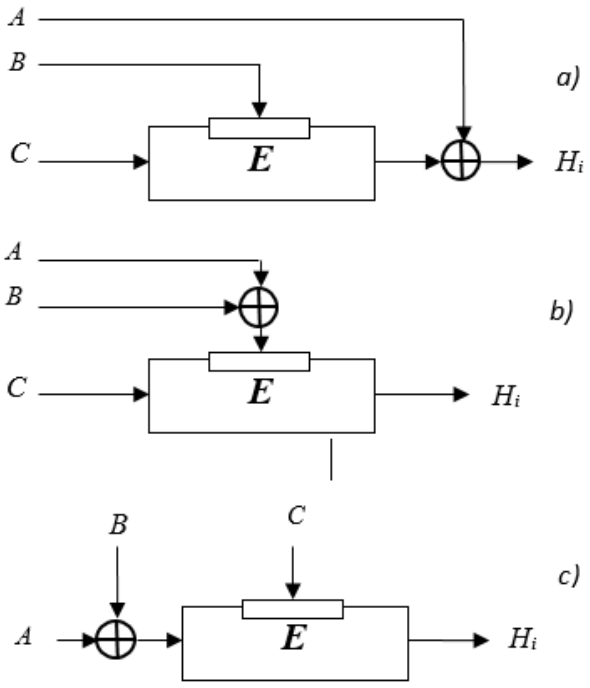
Бугунги кунда блокли шифрлаш алгоритмлар асосида яратилган хеш функцияларда қўлланилган турли хил юқори бардошликка эга блокли шифрлаш алгоритмлар сони етарлича. Умумий ҳолда блокли шифрлаш асосида қурилган хеш функцияларнинг хеш қийматини ҳисоблаш формуласи Rabin схемасида келтирилган бўлиб, у қуйидагича ифодаланади [6].

$$H_i = Э_{Mi}(H_{i-1}), \quad i = 1,2, \ldots\ldots n, \qquad (2)$$

бу ерда: шифрлаш алгоритми индексида қўлланилган M_u калит сифатида ишлатилади.

Бундан ташқари хеш функцияларни яратишда раунд акслантиришларига қўшимча сифатида *XOR* бўйича қўшиш амалидан ҳам фойдаланилади.

2-расмда шундай раунд акслантиришларининг умумий тузилишининг учта турли хил схемаси келтирилган. Шу билан бир қаторда ушбу кўрсатилган вариантларнинг умумлашган схемасидан ҳам фойдаланиш мумкин.



a) Э функциянинг чиқишига қўшилиши,
b) Е функция калитига қўшилиши,
c) Е функциянинг киришига қўшилиши.

2-расм. Раунд хеш функция умумий қурилиш схемасининг вариантлари.

Одатда юқорида кўрсатилган схемалардаги *A, B, C* параметрлар ўрнида H_{i-1}, M_{i-1} ёки M_i қийматларидан фойдаланилади. Тадқиқотлар шуни кўрсатадики, хеш функцияда бардошлилиги юқори бўлган шифрлаш алгоритмидан фойдаланиш, бардошли хеш функция қуришнинг етарли шарти ҳисобланмайди. Шунинг учун хеш функция алгоритмларининг мавжуд криптотаҳлил усулларига бардошлилигини ошириш учун биринчидан, кириш блок узунлиги $m \geq 128$**,** иккинчидан, хеш функциянинг функцияси сифатида танланган *F*-функция умумий ҳолда 2-жадвалдаги формулаларга мос ҳолда хеш функция алгоритмини тузиш мақсадга мувофиқ ҳисобланади [7].

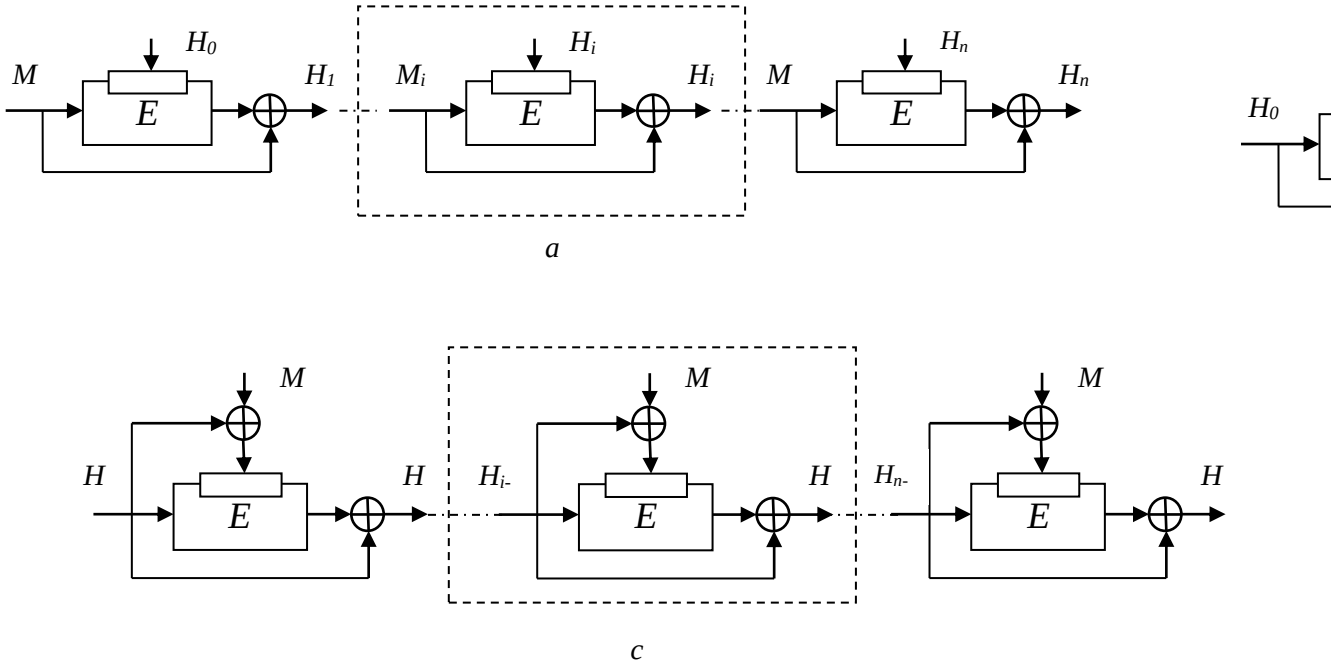
2-жадвал

Бардошли блокли шифрлаш алгоритми Е асосида хеш функция схемаларини қуришнинг мумкин бўлган формулалари

№ t/r	Формула
1.	$H_j = E_{H_{i-1}}(M_i) \oplus M_i$
2.	$H_i = E_{H_{i-1}}(M_i \oplus H_{i-1}) \oplus M_i \oplus H_{i-1}$
3.	$H_i = E_{H_{i-1}}(M_i) \oplus M_i \oplus H_{i-1}$

4.	$H_i = E_{H_{i-1}}(M_i \oplus H_{i-1}) \oplus M_i$
5.	$H_i = E_{M_i}(M_i \oplus H_{i-1}) \oplus H_{i-1}$
6.	$H_i = E_{M_i}(M_i \oplus H_{i-1}) \oplus M_i \oplus H_{i-1}$
7.	$H_i = E_{M_i}(H_{i-1}) \oplus M_i \oplus H_{i-1}$
8.	$H_i = E_{M_i}(M_i \oplus H_{i-1}) \oplus H_{i-1}$
9.	$H_i = E_{M_i \oplus H_{i-1}}(M_i) \oplus M_i$
10.	$H_i = E_{M_i \oplus H_{i-1}}(H_i) \oplus H_{i-1}$
11.	$H_i = E_{M_i \oplus H_{i-1}}(M_i) \oplus H_{i-1}$
12.	$H_i = E_{M_i \oplus H_{i-1}}(H_{i-1}) \oplus M_i$

3-расмда 2-жадвалдаги биринчи, бешинчи ва ўнинчи тартибдаги ҳисоблаш формулалари асосида хеш функцияларни қуришнинг схемалари келтирилган.



3-расм. 2-жадвалдаги 1(a), 5(b), 10(c) ларга мос равишда хеш функция қуришнинг схематик кўринишлари.

Раунд хеш функцияларининг бошқа бир қанча вариантларида ушбу учта H_{i-1}, M_{i-1} ва M_i параметрлардан турлича фойдаланиш орқали ҳам қуриш мумкин. Бундай схемаларда битта ортиқча регистрдан фойдаланилади аммо бу ҳолат янада кўпроқ бардошли схемаларни қуриш имконини беради.

Хеш функцияларни қуришда блокли шифрлашдан ташқари бир томонлама функция лардан ҳам фойдаланилади.

Бир томонлама функция – бу чиқиш қийматига кўра кириш қийматини ҳисоблаш мумкин бўлмаган функциядир.

$$y = F(x) \quad (3)$$

$$x` = G(y)$$

$$x \neq x'$$

бу ерда: f – бир томонлама функция . Масалан: факторизация, дискрет логарифмлаш функциялари бир томонлама функция ҳисобланади.

Бир томонлама функцияни бардошли блокли шифрлаш E – алгоритми ёрдамида ҳам қуриш мумкин. Масалан:

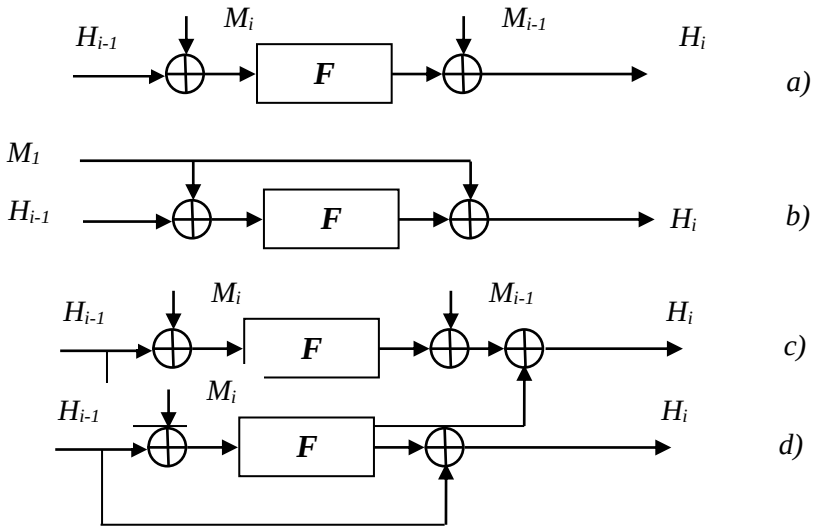
$$F[x] = x \oplus E_k(x) \quad (4)$$

$$F[x,H] = H \oplus E_x(H) - SHA \quad (5)$$

$$F[x,H] = x \oplus E_H(x) - GOST\ 28147\text{-}89 \quad (6)$$

бу ерда: E – (4) ифодада симметрик блокли шифрлаш алгоритми, (5) ва (6) ифодаларда маълум акслантиришлар кетма-кетлиги, k – фиксирланган калит.

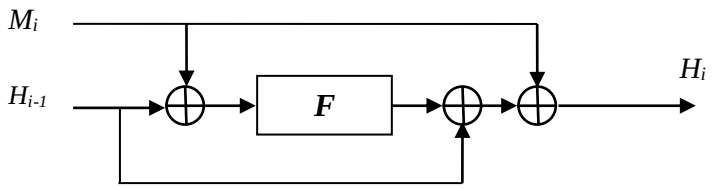
Мазкур усул асосида қурилган хеш функциялар фақатгина кириш ва чиқиш қийматларига эга бўлади. Бу эса, ўз навбатида, уларнинг турли хил схемаларда қўлланилиш имкониятини яратади. Бир томонлама функциялар орқали хеш функцияга қўшимча кириш каналини киритишни осонлаштиради ва 2-жадвалда кўрсатиб ўтилган 12 та формулаларни қўллаш имконини беради. Бундай ҳолатлар 4-расмда келтирилган. (шартли равишда F функциянинг кириш блок узунлиги $m \geq 128$ *бит*).



F - бир томонлама функция

4-расм. Бир томонлама блокли акслантиришлар асосида қурилган хеш функция схемаси.

Юқорида бир томонлама функцияларни блокли шифрлаш алгоритми *E* асосида ҳам қуриш мумкинлиги таъкидланган эди. Амалиётда бир томонлама функциянинг аргументидан кўп маротаба акслантиришга кириш параметри сифатида қўлланилади. Бу эса ҳар доим ҳам бардошликни оширавермайди. масалан 5-расмда 4-расмдаги *(b)* ва *(c)*ларнинг умумлашган схемаси келтирилган.



5-расм. F бардошли функциядан фойдаланган ҳолда тузилган бардошсиз хеш функция.

Ушбу схемадан тузилган хеш функциянинг умумий формуласи қуйидагича.

$$H_i = F(M_i \oplus H_{i-1}) \oplus M_i \oplus H_{i-1} \qquad (7)$$

Қуйида ушбу схема асосида қурилган хеш функция алгоритмига коллизия топиш жараёни кўриб чиқилади.

Айтайлик $M = (M_1, M_2, ...M_n)$ маълумот берилган бўлсин. Юқорида келтирилган формула асосида M маълумотнинг барча оралиқ хеш қийматлари $H_1, H_2, ... H_n$ ларни ҳисоблаб чиқилади. Кейин эса M маълумотнинг айрим блокларидаги маълумот $M_{i+1}, M_{i+2},....M_j$ ларнинг ўринларига бошқа бир $M'_{i+1}, M'_{i+2},....,M'_j$ ларни қўйиб чиқилади. Булар эса мос равишда янги $H'_{i+1}, H'_{i+2},....,H'_j$ қийматларни юзага келтиради. Бундан сўнг эса M'_{j+1} нинг қиймати

$$M`_{j+1} = H_j \oplus H`_j \oplus M_{j+1}$$

билан ҳисоблаб топилган бошқа бир қиймат билан алмаштирилади ва H'_{j+1} ни ҳисобланади.

$$H`_{j+1} = F(M`_{j+1} \oplus H`_j) \oplus M`_{j+1} \oplus H`_j = F(H_j \oplus H`_j \oplus M_{j+1} \oplus H`_j) \oplus$$
$$H_j \quad \oplus H`_j \oplus M_{j+1} \oplus H`_j = F(H_j \oplus M_{j+1}) \oplus H_j \oplus M_{j+1} = H_{j+1} \quad . \tag{8}$$

(8)-ифодадан кўриниб турибдики M_{j+1} маълумот блокининг хеш қиймати H_{j+1}, унинг ўрнига қўйилган M'_{j+1} маълумотнинг хеш қиймати H'_{j+1} билан бир хил. Бу эса $H`_{j+1}$ дан кейинги қадамларда оралиқ хеш қийматларнинг бир хил бўлишини билдиради. Демак M маълумотнинг M'_{j+1} гача қисмини ўзгартириб ҳам ҳудди шундай хеш қийматни ҳосил қилиш мумкин. Натижа

$$H(M') = H(M) = H_n = H. \tag{9}$$

Берилган M маълумот ва унинг хеш қиймати H ни маълум бўлган ҳолда, унга шундай бир бошқа M' ни ҳисоблаш мумкинки, натижада ушбу янги M' нинг ҳам қиймати H га тенг бўлади.

Юқорида хеш функция алгоритмларига қўйиладиган умумий талаблар, хеш функцияларнинг ахборот тизимларида қўлланилиши, хеш функцияларни қуришнинг схемалари, шифрлаш алгоритмлар асосида хеш функцияларни қуриш тамойиллари ва формулалалри ҳақида таҳлиллар натижалари келтириь ўтилди. Мавжуд хеш функция алгоритмлари ва уларнинг яратилиш усуллари ҳамда баҳолаш натижалари, хеш функция алгоритмларини ишлаб чиқиш босқичлари, уларни баҳолашда фойдаланиладиган таҳлил усуллари бўйича уларнинг натижаларини кейинги тадқиқотларда келтириш кўзда тутилган.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР:

1. Akbarov D.A. Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo’llanilishi. – Toshkent, 2009. – 428 b.
2. Алферов А.П. и др. Основы криптографии: учебное пособие. – Москва: Гелиос АРВ, 2002. – 480 с.
3. Бабенко Л.К., Ищукова Е.А. Дифференциальный криптоанализ упрощенной функции хеширования SHA. //Известия ЮФУ. Технические науки, 2010. – № 11. – С.203-219.

4. Вельшенбах М. Криптография на Си и C++ в действии. – Москва: ТРИУМФ, 2004. – 464 с.

5. Кнут Д. Искусство программирования. Т. 2. Получисленные алгоритмы. – Москва: МЦНМО, 1999. – 788 с.

6. Молдовян А.А. и др. Криптография Скоростные шифры. – Санк-Петербург: БХВ-Петербург, 2002. – 494 с.

7. Молдовян Н.А., Молдовян А.А., Еремеев М.А. Криптография: от примитивов к синтезу алгоритмов. – Спб.: БХВ – Петербург, 2004. – 448 с.

8. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – Москва: ТРИУМФ, 2003. – 816 с

9. Babenko L,. Ischukova E. Differential Analysis GOST Encription Algorithm'' Proccedings of the 3 International Conference of Security of Information and Networs (SIN 2012), ACM, New York, 2010. –P.149-157.

10. Federal Information Processing Standards Publication 180-2. Secure Hash Standard. 2002 August 1.

11. Federal Information Processing Standards Publication 198. The Keyed-Hash Message Authentication Code (HMAC). 2002 March 6.

12. Florent Chabaund, Antoine Joux, Differential Collisions of SHA-0 [Электронный ресурс].-19 June, 2000. - http://fchabaund.free.fr/English/Publications/, Свободный.

13. Krystian Matusiewicz, M.Sc. Analysis of Modern Dedicated Cryptographic Hash Functions. – Macquarie University, 2007. – 153 b.

14. NESSIE consortium, "NESSIE Security report." Deliverable report D20 – NESSIE, 2002. – [Electronic resource] – Access mode: http://www.cryptonessie.org/.

15. http://codeproject.com