АҚПАРАТТЫҚ ЖҮЙЕЛЕР
ИНФОРМАЦИОННЫЕ СИСТЕМЫ
INFORMATION SYSTEMS

DOI 10.51885/1561-4212_2024_2_198
МҒТАА 81.93.29

А. Хомпыш[1,2], О.А. Лизунов[2]
[1]Нұр-Мүбарак Египет ислам мәдениеті университеті, Алматы қ., Қазақстан
*E-mail: ardabek@mail.ru**
[2]Ақпараттық және есептеуіш технологиялар институты, Алматы қ., Қазақстан
E-mail: o.lizunov@bk.ru

IoT ҚҰРЫЛҒЫЛАРЫНА АРНАЛҒАН ЖЕҢІЛСАЛМАҚТЫ ШИФРЛАУ АЛГОРИТМІ

ЛЕГКОВЕСНЫЙ АЛГОРИТМ ШИФРОВАНИЯ ДЛЯ УСТРОЙСТВ IoT

LIGHTWEIGHT ENCRYPTION ALGORITHM FOR IoT DEVICES

Аңдатпа. *Бұл мақалада шекті ресурстарға негізделген аппаратты құрылғылардағы мәліметтерді қорғауға арналған жаңа жеңілсалмақты шифрлау ISL_LWC алгоритмі ұсынылған. Ұсынылған жеңілсалмақты шифрлау ISL_LWC алгоритмін зерттеу, Speck және Present алгоритмдерімен салыстыру барысында Arduino Uno R3 платасы қолданылды. Барлық үш жеңілсалмақты шифрлау алгоритмдерінің шифрлау жылдамдығын және раундттық кілттерді генерациялау көрсеткіштерінің сапасын зерттеу үшін алгоритмдер жоғарыдеңгейлі C++ бағдарламалау тілінде бағдарламалық жүзеге асырылды. Шифрлау жылдамдығын және раундттық кілттерді генерациялау жылдамдығын тексеру Arduino Uno R3 платасы негізінде АҚШ-тың Ұлттық стандартты және технологиялар институты дайындаған платформадағы бағдарламалық кіріс кодтары алынып осы негізінде тесттер жүргізілді. Зерттеу жүргізу барысында мақсатқа сай қанағаттанарлық нәтиже алынды. ISL_LWC шифрлау алгоритмі шекті ресурстардағы аппараттық құрылғыларға қолдануға жылдамдығы жағынан сипаттамалық талаптарға сәйкес келетіндігі анықталды. Сонымен қатар S блоктың қасиеттері зерттеліп нәтижелері ұсынылды.*

Түйін сөздер: *Жеңілсалмақты криптографиялық алгоритмдер, Arduino Uno R3, ISL_LWC, IoT құрылғылары, раундттық кілт, бағдарлама, ауыстыру, сызықты емес түрлендірулер, микроконтроллер, шифрлау, NIST, S-box, шифрлау алгоритмі.*

Аннотация. *В данной статье представлен новый легковесный алгоритм шифрования ISL_LWC, предназначенный для защиты данных на устройствах с ограниченными аппаратными ресурсами. Для проведения исследования и сравнительного анализа разработанного легковесного алгоритма шифрования ISL_LWC с алгоритмами Speck и Present была использована плата Arduino Uno R3. Все три легковесных алгоритма шифрования были реализованы на высокоуровневом языке программирования C++. В качестве исследуемых показателей были взяты скорость зашифрования и генерации раундовых ключей. Для проведения тестов по измерению скорости зашифрования и генерации раундовых ключей на базе платы Arduino Uno R3 были взяты исходные коды программной платформы, подготовленной Национальным институтом стандартов и технологий США для этих целей. В целом, полученные результаты проведенных исследований – удовлетворительные. Алгоритм шифрования ISL_LWC по своим скоростным характеристикам соответствует требованиям, предъявляемым к алгоритмам шифрования, используемым в устройствах с ограниченными аппаратными ресурсами. Также были изучены свойства S блока и представлены результаты.*

Ключевые слова: *Легковесные криптографические алгоритмы, Arduino Uno R3, ISL_LWC, устройства IoT, раундовый ключ, программное обеспечение, перестановка, нелинейные преобразования, микроконтроллер, шифрование, NIST, S-box, алгоритм шифрования.*

Abstract. *This article introduces a novel lightweight encryption algorithm called ISL_LWC, which aims to secure data on devices with constrained hardware capabilities. To perform a research study and conduct a comparative analysis between the newly developed ISL_LWC encryption algorithm and the*

existing Speck and Present algorithms, an Arduino Uno R3 board was utilized. All three lightweight encryption algorithms were implemented using the high-level C++ programming language. The speed of encryption and generation of round keys were taken as the studied indicators. In order to evaluate the encryption speed and generate round keys on the Arduino Uno R3 board, the software platform provided by the US NIST was utilized. The source codes from this platform were employed for the tests. Overall, the conducted studies yielded satisfactory outcomes. The speed characteristics of the ISL_LWC encryption algorithm were found to fulfill the requirements for encryption algorithms employed in devices with restricted hardware resources. The properties of block S were also studied and the results were presented.

Keywords: *lightweight cryptographic algorithms, Arduino Uno R3, ISL_LWC, IoT devices, round key, software, permutation, non-linear transformations, microcontroller, encryption, NIST, S-box, encryption algorithm.*

Кіріспе. Соңғы жылдары жаңа технологиялардың қарқынды дамуы нәтижесінде шағын шекті ресустарга негізделген құрылғылар пайда болды. Заманауи мұндай технологиялар қазіргі уақытта әртүрлі салаларда кең қолданысқа ие. Бұл технологияларды қолданудың ерекшеліктері кейбір мәселелерді жылдам, қолайлы шешуге мүмкіндік беретін технологияга айналды. Айта кететін болсақ шекті ресурстарга негізделген құрылғыларга келесілерді жатқызуга болады. Олар: IoT, RFID және смарт технологиялар қолданысқа ие [1, 2].

Қазіргі уақытта интернет желісі арқылы мұндай технологияларды пайдалану арқылы әртүрлі қызметтерді пайдалану күрт өсуінің нәтижесінде оларга жасалатын шабулдардың көбейгендігі белгілі. Ал шекті ресурстарга негізделген мұндай технологиялардың қауінсіздігін қамтамасыз ету дәстүрлі криптографиялық әдістер үшін тиімсіз болып табылады. Себебі дәстүрлі криптографиялық қоргау алгоритмдері блок ұзындыгының жогару болуы және құрамындагы криптографиялық түрлендіру әдістерінің күрделілігі өз кезегінде мұндай құрылғылардың жұмыс істеуіне қолайсыз болып табылады. Сондықтан шекті ресурстарга негізделген технологиялардың қауінсіздігін қамтамасыз ететін алгоритмдерді жасау өзекті мәселердің бірі болып табылады. Шекті ресурстарга негізделген криптографиялық алгоритмдерді жеңілсалмақты криптографиялық алгоритмдер деп атаймыз. АҚШ-тың, Ұлттық стандарттар және технологиялар институты (ҰСТИ агл. NIST) 2021 жылы алгашқы жеңілсалмақты шифрлау алгоритмдері туралы конкурс жариялады [3,4]. Конкурсқа 20-дан астам алгоритмдер қатысты солардың ішінде 2012 ж. Present [5] және Clefia [6] шифрлау алгоритмдері жеңімпаз атанып NIST шешімі бойынша жеңілсалмақты криптографиялық алгоритмдердің стандарты болып бекітілді.

Present шифрлау алгоритмінің сипаттамасы блок ұзындыгы 64 бит, раундттардың саны 32, құрылымы Фейстель желісі негізінде жасалынган. Алгоритмнің құрылымында 4х4 өлшемді сызықты емес S блок және сызықты P блок биттік орын ауыстыру криптографиялық түрлендіру операциясы орындалады. Соңгы жылдары жеңілсалмақты шифрлау алгоритмдерге байланысты NIST өздерінің жаңа талаптарын қоса отырып конкурс жариялады. Сонымен қатар жеңілсалмақты шифрлау алгоритмдердің жылдамдықтарын сынақтан өткізу үшін арнайы багдарламалық қамтамасыз ету платформаларын даярлап ұсынды [7].

NIST жеңілсалмақты крипторгафиялық алгоритмдердің құрамындагы криптографиялық түрлендіру әдістері үшін жалпы талап етілетін негізгі критерийлер ретінде келесілерді айтуга болады [8]. Олар:

- Сенімділігі: Жеңілсалмақты шифрлау алгоритмдерінің криптошабулдарга төзімділік деңгейі қамтамасыз етілуі керек. Әдетте сенімділік деңгейі 2^{112} кем болмауы керек.

- Икемділігі: Алгоритм әртүрлі платформаларга ыңгайлы іске асырылуы керек. Сонымен қатар бір платформада әртүрлі қызметтерді орындай алатындай болу керек. Блок және кілт өлшемдері сияқты параметрлерді орындау үшін ортақ түрлендіру әдістері қолданылмайтын әртүрлі алгоритмдерді салыстыруга мүмкіндік беруі керек.

- Бірнеше түрлендірулер үшін төмен шығындар: Бір ғана құрылымды пайдалана отырып әртүрлі түрлендіру әдістерін қолдану (мысалы, шифрлау және шифрды ашу) мүмкіндігін беретін алгоритмдер жасай отырып басқада алгоритмтердің құрылымындағы түрлендірулерге қарағанда мүлдем басқа құрылымда жақсырақ нәтиже беретін шекті құрылғыларға аз шығынды беретін түрлендіру әдісі болуы керек.

- Шифрмәтіннің өлшемі: Шифрмәтіннің өлшемі аппараттық ресурстарға қажетті мәліметтерді сақтау және жіберу үшін әсер етеді. Сондықтан шифрлау алгоритмдерінің шифрлау нәтижесінде ашықмәтіннен ұзын емес шифрмәтіндердің болғаны дұрыс, өйткені ол сақтау және тасымалдау талаптарын азайтуға көмектеседі.

- Кездейсоқ арналық шабуылдар мен сәтсіздіктерге төзімділік: Бұл талап негізінен IoT құрылғылары үшін өте маңызды, себебі қасқүнемдер құрылғыларға физикалық тұрғыдан қол жеткізе алады. Ал ресурстар шектеулі болғандықтан, мұндай шабуылдарды азайтуға қарсы шаралар жүргізу арқылы жетімді болмауын қадағалау керек.

- Ашықмәтін/шифрмәтін жұптарының санына шектеулер: Алгоритм жасаушылар бір команда арқылы түрлендіруге болатын ашықмәтін/шифрмәтін жұптарының санының жоғарғы шегін орнатуға рұқсат етуі мүмкін. Ол криптографиялық алгоритмдегі шекті құрылғының шектеулеріне ыңғайлы және нақты қолданбаның талаптарына сәйкестендіруге мүмкіндік береді.

- Кілтке қатысты шабуылдарға төзімділік: Бұл негізінен криптографиялық алгоритмдердің негізгі өзекті талаптарының бірі болғандықтан, кілттерді пседокездейсоқ генератордан алыну керек.

Ақпараттық және есептеуіш технологиялар институтындағы Ақпараттық қауінсіздік зертханасында гранттық жоба негізінде жасалынып отырған бұл алгоритмді жасау барысында осы аралыққа дейінгі шекті құрылғыларға негізделген жеңілсалмақты шифрлау алгоритмдердің құрамын зерттей отырып нәтижесінде жаңа шифрлау ISL_LWS алгоритмі ұсынылды.

Бұл ұсынылып отырған жеңілсалмақты шифрлау алгоритмінің жылдамдығын тексеру үшін аппараттық ресурстардағы шекті ресурстарға арналған құрылғылардың талаптарына жауап беретін құрылғы пайдаланылды.

Шекті құрылғыларға негізделген жеңілсалмақты шифрлау алгоритмдері бойынша жүргізілген зерттеулерге сай келесі жұмысты атап өтуге болады. Бұл жұмыстарда авторлар белгілі шифрлау алгоритмдерінің құрамындағы әртүрлі түрлендіру әдістерінің ерекшеліктерін сиппатаған және алгоритмнің жылдамдығын тексеру үшін алгоритмді багдарламалықта жүзеге асыра отырып зерттеген [9,10]. Мысалы, Бабенко Л.К., Голотина Д.В., Макаревич О.Б. [11] Trivium [12] ағындық шифрының сипаттамасын және оның аппараттық жүзеге асырылу процессі туралы зертеулерін жүргізген. Онда Trivium шифры багдарламалық жүзеге асырудан қараганда аппараттық құралдарға негізделген алгоритм екендігін анықтаған. Сонымен қатар авторлар зерттеу жұмыстарын жүргізу барысында бұл шифр FPGA, Marsohod 2Bis тақтасында жүзеге асырылғандығын және әзірленген алгоритм бұл мобильді роботтармен жұмыс істеу кезінде пайдалануға болатындығын көрсеткен [10].

Келесі жұмыста мақала авторы Л.К. Бабенко және т.б. Present шифрын зерттеген [13,5]. Онда авторлар алгоритмнің багдарламалық қамтамасыз етуді іске асыруды жүзеге асыра отырып, сонымен қатар чиптегі жүйеге арналған арнайы әзірленген аппараттық блокты өндеген. Бұл әзірлеме шекті ресурсты криптография талаптарына сәйкес келетіндігін және әртүрлі құрылғыларда іске асыруда оңтайлы шешім болатындығы айтылған [14]. Ал Жуков [15] және Tang, Zh [5] еңбектерінде шекті құрылғыларға негізделген Present, Trivium және Clefia сияқты шифрларды зерттей отырып зерттеу нәтижелеріне ұсынған. Онда Clefia алгоритмі басқа алгоритмдерге қараганда жылдамы-

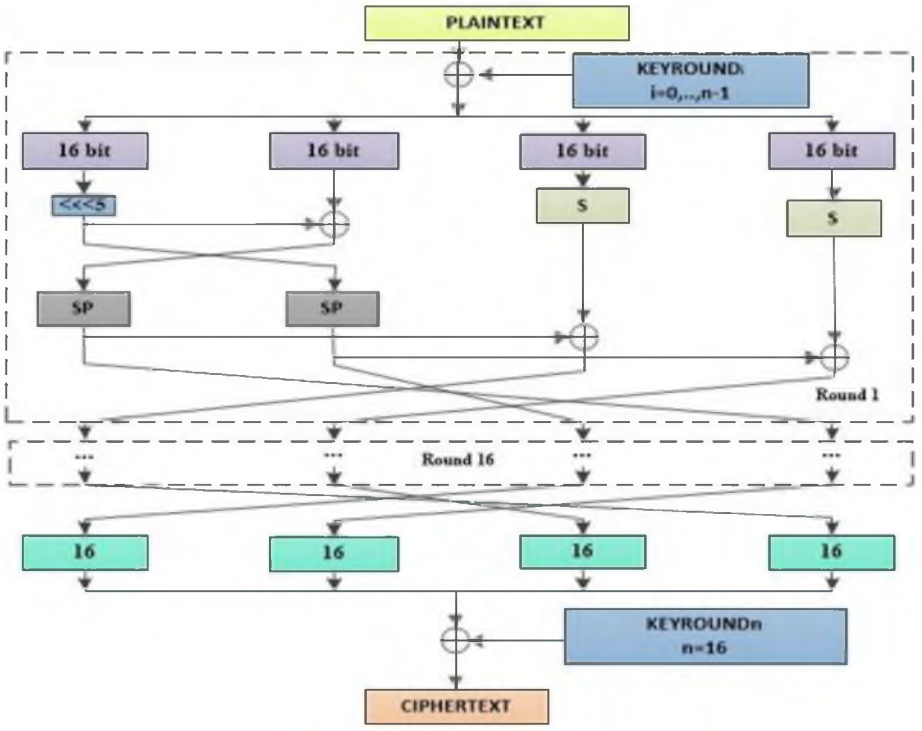
рақ сонымен қатар мобильді робототехникада шифрлау үшін қолдануға ыңғайлы нұсқасы деп көрсеткен. Ал Present шифры бағдарламалық жасақтамада енгізілгенде шифрлау жылдамдығы төмен болатындығы айтылған. Бұл зерттелініп отырған Present және Trivium алгоритмде аппараттық құралдарға негізделген шифрлар болып табылады.

Бұл мақалада сонымен қатар ұсынылып отырған ISL_LWC жеңілсалмақты шифрлау алгоритмінің жылдамдығын тексеру барысында Arduino Uno R3 тақтасы таңдалды.

Материалдар және зерттеу әдістері. ISL_LWC шифрлау алгоритмінің құрылымы. Криптографиялық жеңілсалмақты шифрлау алгоритмдеріне талдау жүргізіле отырып, ол алгоритмдердің құрылымдағы әрбір түрлендіру әдістерінің ерекшеліктерін зерттей келе ISL_LWC шифрлау алгоритмі ұсынылды. Бұл алгоритм шекті ресустарға негізделген құрылғыларға арналған алгоритм болып табылады. ISL_LWC алгоритмі жеңілсалмақты симметриялық блокты алгоритмның құрамына жатады және ISL_LWC алгоритм келесі негізгі параметрлерден тұрады:

- Мастер кілттің ұзындығы – 80 бит.
- Блоктың ұзындығы – 64 бит.
- Раундттық кілттің ұзындығы – 64 бит.
- Раундтардың саны – 16.

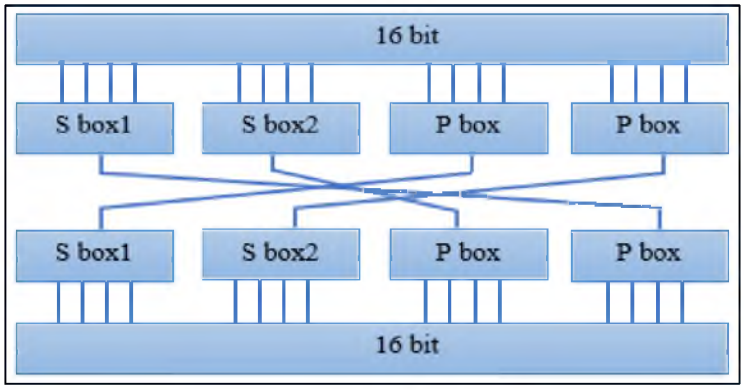
ISL_LWC алгоритмінің шифрлау жылдамдығын және криптоберіктілігін қамтамасыз ету мақсатында модуль екі бойынша қосу операциясы (XOR), SP түрлендіруі, биттік солға жылжыту операциясы, P биттік алмасатыру және S блок орын ауыстыру операциялары қолданылды. Ұсынылып отырған ISL_LWC жеңілсалмақты шифрлау алгоритмінің шифрлау схемасы 1-суретте көрсетілген.



1-сурет. ISL_LWC алгоритмінің шифрлау схемасы

SP түрлендіру әдісі. SP түрлендіру әдісінің құрылымы 2-суретте көрсетілген. Мұнда төрт биттік сызықты емес S box1 (1-кесте) және S box2 (2-кесте) орын ауыстыру және P

box (3-кесте) биттік алматыру әдісі қолданылады. Жоғарыда көрсетілген түрлендіруден өткеннен кейін 2-суретке сәйкес жарты байттық орын ауыстырулар орындалады.



2-сурет. SP түрлендіру әдісі

1-кесте. S box 1 орын ауыстыру кестесі

Input	F	C	A	9	1	E	4	D	5	7	8	6	0	2	B	3
Output	C	0	4	3	E	7	8	F	A	1	5	B	2	D	9	6

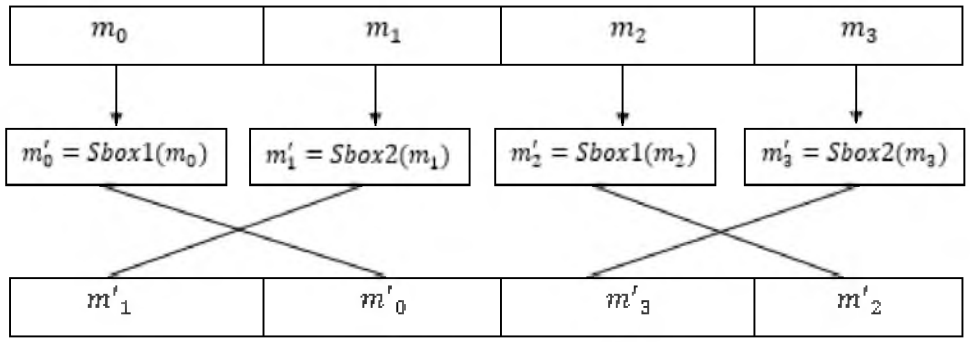
2-кесте. S box 2 орын ауыстыру кестесі

Input	E	C	F	9	3	B	4	8	6	A	2	7	5	1	D	0
Output	1	7	B	9	8	A	C	0	4	6	D	E	2	5	3	F

3-кесте. P box биттік алмастыру

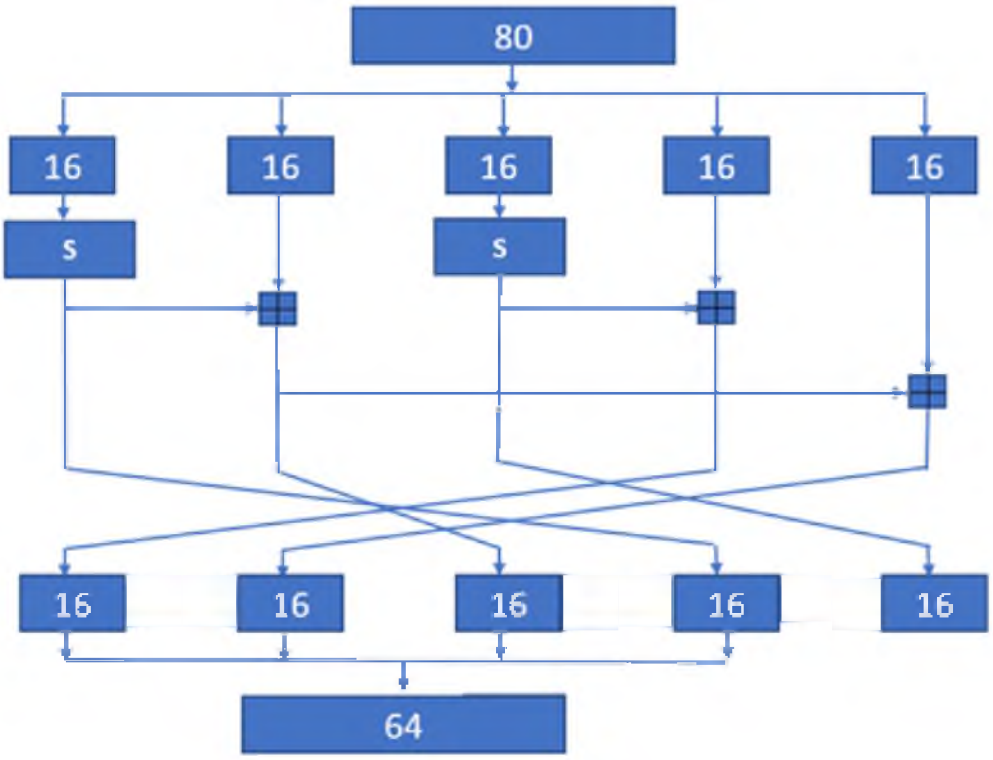
j	1	0	3	2
P(j)	2	3	1	0

S түрлендіру әдісі. Ашық мәтіннің кіріс 16 биті келесідей өрнектеліп алынады: $a_0a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}a_{11}a_{12}a_{13}a_{14}a_{15}$. Мұндағы әрбір 4 битті жеке жарты байт ретінде аламыз, яғни: $m_0 = a_0a_1a_2a_3$, $m_1 = a_4a_5a_6a_7$, $m_2 = a_8a_9a_{10}a_{11}$, $m_3 = a_{12}a_{13}a_{14}a_{15}$, мұндағы m_i, $i = \overline{0,3}$. Ары қарай 3-суретке сәйкес m_0, m_2 және m_1, m_3 4-биттік S box1 және S box2 ауыстыру кестесінен өтеді және орын алмастырылады.



3-сурет. S түрлендіру әдісі

Раундттық кілттерді генерациялау алгоритмі. Блокты алгоритмдерінің маңызды элементтерінің бірі раундттық кілт екендігін ескере отырып, раундттық кілттер жасау алгоритмі ұсынылды. Онда алгоритмнің негізгі кілт ұзындыгы 80 битке тең және ұзындыгы 16 бит болатындай бес ішкі блоктарга бөліну арқылы 4-суретке сәйкес орындалды. Алгоритмнің құрамында S-блок және модуль бойынша қосу операциялары орындалады. Әрбір операциялар өз кезегінде сапалы кілттерді жасауга мүмкіндік береді.



4-сурет. Раундттық кілт генерациялау алгоритмі

Бұл мақаладагы жұмыстың басты мақсаты ұсынылып отырган ISL_LWC жеңілсалмақты шифрлау алгоритмнің жылдамдыгын Arduino Uno board платформасында және багдарламалық тексеру болып табылады. Себебі блокты шифрлау алгоритмдеріне қойылатын талаптардың біріне сәйкес алгоритм жылдамдыгы жогары болу керек.

Зерттеу нәтижелері және оларды талқылау. Деректерді криптографиялық қоргау алгоритмдері багдарламалық және аппараттық құралда да жүзеге асырылады. Алгоримтмді аппараттық құралдарда жүзеге асыру айтарлықтай қымбат, бірақ оның тиімділігі артықшылықтары өте көп. Ал криптографиялық алгоритмдерді багдарламалық жүзеге асыру айтарлықтай жаңалық емес, бірақ аппараттық жүзеге асырудан қараганда аз шыгынды талап етеді және алгоритм құрамына қандайда өзгертулер енгізу жагынан тиімді қызметтер атқарады. Бұл мақалада қазіргі уақыттагы қол жетімді Arduino UNO платформасын пайдалана ISL_LWC жеңілсалмақты шифрлау алгоритмнің жылдамдыгы анықталады. Бірақ зерттеу жұмысының негізгі объектісі шекті құрылгыларга арналган платформа үшін әзірленген алгоритмнің өзі болып саналады [16].

Ұсынылып отырган ISL_LWC жеңілсалмақты шифрлау алгоритмінің жылдамдыгын аппаратты түрде багалау Arduino UNO тақтасында жүргізілді (5-сурет).

Arduino UNO тақтасының негізгі сипаттамалары төменде көрсетілген:

1. Микроконтроллер – ATmega 328.
2. Жиілігі – 16 MHz.
3. Кернеуі – 5 V.
4. Флэш жады – 32 MB.

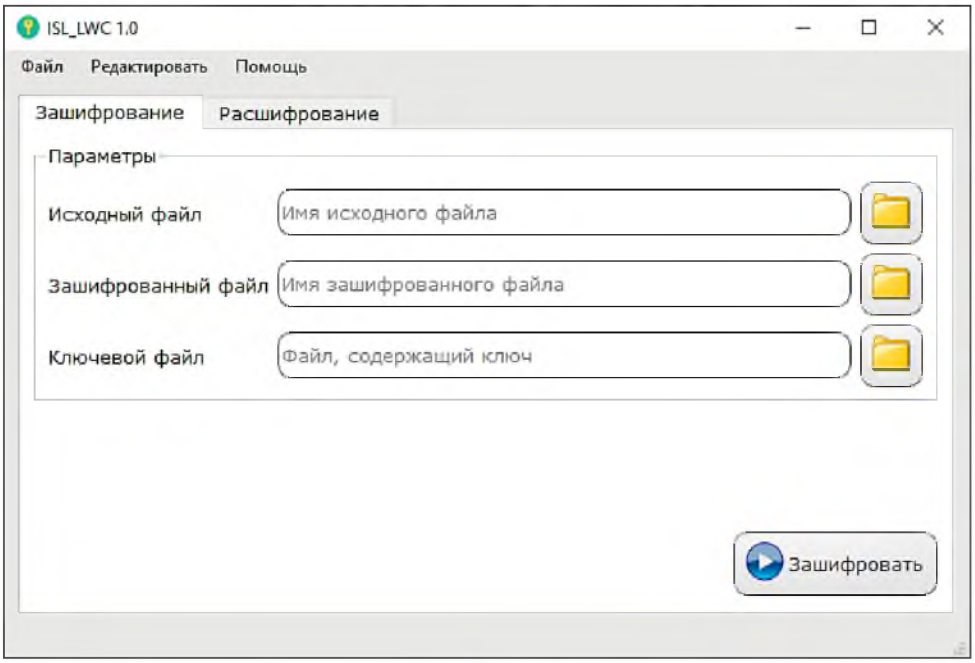
5-сурет. Arduino Uno R3 тақтасы

ISL_LWC шифрлау алгоритмі Visual Studio 2013 C++ бағдарламалау тілінде және арнайы Arduino IDE кітапханасына негізделе отырып жазылды. Сонымен қатар алгоритмнің жылдамдықтарын салыстыру үшін белгілі Present, Speck алгоритмдерінде бағдарламалық және Arduino IDE платформасында арнайы жазылып салыстырулар жүргізілді. ISL_LWC алгоритмінің зерттелген салыстырмалы нәтижелері 4-кестеде көрсетілген.

4-кесте. ISL_LWC алгоритмінің салыстармалы нәтижелері

Параметрлері	Жеңілсалмақты шифрлау алгоритмдері		
	Present	Speck	ISL_LWC
Негізгі кілт ұзындығы (bit)	80	96	80
Ашықмәтін блок ұзындығы (bit)	64	64	64
Шифрлау уақыты (μs)	2111,56	16,90	108,59
Раундттық кілт жасау уақыты (μs)	1541,31	1320,69	275,12

ISL_LWC шифрлау алгоритмінің бағдарламалық сипаттамасы. Мақаладағы ISL_LWC шифрлау алгоритмінің Visual Studio 2013 C++ бағдарламалау тілінде жүзеге асырылған бағдарламасы "ISL_LWC 1.0" файлдарды шифрлау атауымен аталынып арнай авторлық құқық куәлігі алынды. Бағдарламаның негізгі беті 6-суретте көрсетілген.



6-сурет. ISL_LWC алгоритмінің шифрлау бағдарламасы

Жеңілсалмақты шифрлау алгоритмдерінің жылдамдығын салыстыру мақсатында 25,5 МБ өлшемді .pdf файлы таңдалып алынды. Таңдалған файлды Present, Speck, ISL_LWC алгоритмі арқылы шифрлап және шифрланған файлдың уақыттары салыстырылды (5-кесте).

5-кесте. Алгоритмдердің шифрлау жылдамдығының салыстырмалы нәтижесі

Жеңілсалмақты шифрлау алгоритмдері	Файл өлшемі	Шифрлау жылдамдығы	Жүзеге асырылған компьютердің сипаттамасы
Present	25,5 Mb	5,13 сек	Intel(R) Core(TM) i7-10700 CPU @ 2.90GHz 2.90 GHz RAM 16Gb, Windows 10 64bit
Speck		1,20 сек	
ISL_LWC		1,33 сек	

S блоктың қасиеттерін зерттеу нәтижесі. ISL_LWC алгоритмінің құрамындағы маңызды түрлендіру әдістерінің бірі 1-кесте және 2-кестеде көрсетілген S блоктар екендігіні белгілі. Себебі бұл алгоритмнің криптоберіктілігіне жауап беретін негізгі түрлендіру әдісі болып табылады. Ал S блокты зерттеудің әртүрлі әдістері бар солардың бірі оның қасиеттерін зерттеу болып табылады. S блоктың қасиеттеріне хэмминг салмағын, хэмминг қашықтыгы, сызықсыздық минималды және максималды мәні, корреляциялық минималды және максималды мәні, автокорреляциялық минималды және максималды мәні, теңестірілген немесе теңестірілмеген, SSI (sum-of-squares indicator) мәні [17, 18].

Енді жоғарыда ұсынылып сипаттамалардың негізгі ұғымдары мен анықтамаларына тоқталсақ. Теңестірілген деп Бульдік функцияның ақиқаттар кестесіндегі мәндер жиынындағы «0» мен «1»-дің тең болуы: $hw(f) = 2^{n-1}$.

Аффиндық функция деп $f = a_1x_1 \oplus a_2x_2 \oplus a_3x_3 \oplus \dots \oplus a_nx_n$, $a_i \in GF(2)$, $i = \overline{1,n}$ түрде берілген бірінші дәрежелі алгебралық қалыпты форманы айтамызы, егер $a_1 = 0$ болса, онда f функциясы сызықты деп аталады.

α векторының Хэмминг салмағы деп тізбектегі бірліктер саны және ол $hw(\alpha)$ түрінде белгіленеді: $hw(\alpha) = \sum_{x=1}^{2^n} f(\alpha)$.

Хэмминг қашықтығы $hd(f,g)$ деп екі тізбектің сәйкес келетін позициядағы тең болмайтын мәндерінің саны (ягни нөлдік емес вертикалды биграммалар саны), мұндағы $hd(f,g)$ – f және g функцияларының сәйкес позициядағы тең емес мәндерінің саны: $hd(f,g) = \sum_{x=1}^{2^n} f(x) \oplus g(x)$.

N_s түрлендіруінің сызықсыздығы деп S түрлендіруінің шығыс тізбегі мен өрістегі барлық аффиндық функциялардың шығыс тізбектерінің арасындағы ең кіші мәнді айтамыз Хэмминг (минималды) қашықтығы келесі формула бойынша есептеледі:
$N_s = \min\{d(S,l)\}$, мұндағы l – аффиндық функциялар жиыны.

N_f функцияның сызықсыздығы деп f функциясы мен $GF(2^n)$ өрісіндегі барлық аффиндық функциялардың арасындағы ең кіші Хэмминг қашықтығы:
$N_f = \min\{hd(f,\varphi)\}$, мұндағы φ – аффиндық функциялар жиыны.

Бульдік функциясының алгебралық қалыпты формасы деп (Жегалкин көпмүшелігі) келесі өрнекті айтамыз: $f(x_1, x_2, \dots, n) = a_0 \oplus a_1x_1 \oplus a_2x_2 \oplus a_3x_3 \oplus \dots \oplus a_nx_n \oplus a_{12}x_1x_2 \oplus a_{i..i+j}x_i \dots x_{i+j} \oplus \dots \oplus a_{12\dots n}x_1x_2 \dots x_n$, $a_i \in GF(2)$, $i = \overline{0,n}$. Бульдік функцияның дәрежесі деп алгребралық қалыпты форманың (АҚФ) коэффициенті нөлден өзгеше мономдардың ең жоғары дәрежесі айтылады.

$GF(2^n)$ өрісіндегі f функциясының $F(w)$ Уолш түрлендіруі $F(W) = 2^{-n}\sum_x(-1)^{f(x)\oplus\langle\varphi,x\rangle}$ функциясының нақты мәндерді қабылдауымен анықталады, мұндағы $\langle\varphi,x\rangle$ – скаляр көбейтінді.

$f(x)$ бульдік функциясы мен барлық сызықты функциялар жиыны арасындағы корреляциялық мән Уолш түрлендіруі ретінде анықталады: $W(\varphi) = \sum_{x=1}^{2^n}(-1)^{f(x)\oplus\langle\varphi,x\rangle}$.

$r_f(\alpha)$ автокорреляциялық функциясы $f(x)$ бульдік функциясының ақиқаттар кестесіндегі $\alpha \in GF(2^n)$ бағытындағы барлық айнымалылар үшін функцияның туындысы болып табылады және келесідей түрде беріледі: $r_f(\alpha) = \sum_{x=1}^{2^n}(-1)^{f(x)\oplus f(x\oplus\alpha)}$. $r_f(\alpha)$автокорреляциялық функция – $f(x)$ функциясы α орынга жылжытқанда өзінен қаншалықты өзгеретінін білдіреді, басқаша оны индикатор деп атаймыз [19].

Автокорреляциялық функцияның максималды абсолютті мәні келесідей анықталады: $|AC|_{max} = max_\alpha|r_f(\alpha)|$.

Ал SSI «квадраттар қосындылары» келесі формуламен анықталынады (sum-of-square indictors): $\sigma = \sum_{x=1}^{2^n} r_f^2(\alpha)$.

Ұсынылып отырған алгоритмнің құрамындағы S блокты Бульдік функциялардың қасиеттері негізінде зерттелген және Present алгоритмінің S блогының салыстырмалы нәтижелері 6-кестеде көрсетілген. Жоғарыда көрсетіліген S блоктың қасиеттерінің жақсы нәтиже көрсетуі шифрлау алгоритмдерінің криптоберіктілігіне әсер ететін критерийлердің бірі болып табылады.

Егерде S блоктың сызықсыздық анықталаса онда алгоритмге шабул жасаушы тарапынан қандайда бір осальдылықты табу қиынга түсетіні белгілі. Себебі алгоритмге жүргізілетін сызықты криптоталдау нәтижесіндегі алынган мәндер, S блоктың

сызықсыздыгана тікелей байланысты алынады. Сызықсыздық минималды/ максималды мәні төрт биттік S блок үшін 8-ге жақын болган сайын жогары нәтиже көрсетеді. Бірақ зерттеу нәтижесіндегі мәндерді нашар деп айтуга негізсіз. Олардан алынган мәндерден басқа алгоритмнің криптоберіктілігіне жауап беретін криптографиялық түрлендірулердің нәтижелер әсер етеді. Ал теңестірілген нәтижесінде «0» мен «1»-дің тең болуы алгоритмнің лавиндік әсерінің жогары болгандыгын көрсетеді. Алгоримтде лавиндік әсерінің жогары болу нәтижесі статистикалық багалуда және дифференңиальды криптоталдаудың жақсы нәтиже көрсетуінің критерийлерінің бірі болып табылады.

6-кесте. S блоктың қасиеттерінің салыстырмалы нәтижесі

№	S блоктың қасиеттері	Алгоритмдер		
		ISL_LWC		Present
		S box 1	S box 2	
1	Хэмминг салмагын	8	8	8
2	Хэмминг қашықтыгы	8	8	8
3	Сызықсыздық минималды / максималды мәні	4/14	4/14	4/12
4	Корреляңиялық минималды / максималды мәні	-12/8	-12/8	-8/8
5	Автокорреляңиялық минималды / максималды мәні	-16/8	-16/8	-16/16
6	Теңестірілген	иә	иә	иә
7	SSI минималды / максималды мәні	640/1408	640/1408	640/1024

Қорытынды. Қорытындылай келе, қазір уақыттагы жаңарган технологиялардың талаптарына сай келетін ақпаратты қоргау алгоритмдерін жасау өзекті болып табылады. Бұл мақалада шекті құрылгылардагы ақпараттарды қоргауга арналган жаңа ISL_LWC шифрлау алгоритмі жүзеге асырылды. Алгоритмнің құрамындагы әрбір түрлендірулерге сипаттама беріліп атқаратын негізгі мақсаты сипатталган. Сонымен қатар ISL_LWC шифрлау алгоритмінің файлдарды шифрлау жылдамдыгын тексеру аппаратты түрде жүзеге асыру үшін Arduino Uno R3 тақтасы және Visual Studio 2013 C++ багдарламалау тілінде жүзеге асырылды. Салыстыру қазіргі уақыттагы NIST стандарттарын кіретін Present, Speck алгоритмдері арқылы жүргізілді. Зерттеу нәтижелеріне сай ұсынылып отырган ISL_LWC шифрлау алгоритмің құрамындагы қолданылган түрлендірулер жылдам жұмыс жасайтындыгы NIST талаптарына сай келетіндігі анықталды. Сонымен қатар сызықты емес түрлендіру S блоктың қасиеттері зерттелінін салыстырма талдау жүргізілді. Хэмминг салмагы теңестірілгендігі және хэмминг қашықтыгының 8-ге тең болуы S блоктың шыгыс мәніндегі тізбектің жақсы шашыратылганын көрсетеді, ягни «0» мен «1»-дің саны тең. Ал сызықсыздық минималды/ максималды мәні, корреляңиялық минималды / максималды, SSI минималды / максималды мән нәтижелерінде ауытқулар анықталган бірақ ауытқулар нашар S блок дегенді білдірмейді. Жалпы алынган нәтижелер S блокқа қойылатын талаптарды қанагаттандырады. Алгоритмнің криптоберіктілігі келесі зерттеу жұмыстарында зерттелінін нәтижелері ұсынылатын болады.

Алгыс. Бұл мақаладагы зерттеу жұмыстар ҚР ҒжЖБМ AP09259570 «Шектелген ресурстар үшін отандық жеңілсалмақты шифрлау алгоритмін құру және зерттеу»гранттық жоба негізінде жүзеге асырылды.

Әдебиеттер тізімі

1. El-hajj M, Mousawi H, Fadlallah A. Analysis of Lightweight Cryptographic Algorithms on IoT Hardware Platform. Future Internet. 2023; 15(2):54. https://doi.org/10.3390/fi15020054
2. Podimatas P, Limniotis K. Evaluating the Performance of Lightweight Ciphers in Constrained Environments – The Case of Saturnin. Signals. 2022; 3(1):86-94. https://doi.org/10.3390/signals3010007
3. Hanacek, N. (2023). NIST Selects 'Lightweight Cryptography' Algorithms to Protect Small Devices. https://www.nist.gov/news-events/news/2023/02/nist-selects-lightweight-cryptography-algorithms-protect-small-devices
4. Hasan, H., Ali, G., Elmedany, W., Balakrishna C. (2022) Lightweight Encryption Algorithms for Internet of Things: A Review on Security and Performance Aspects [International Conference on Innovation and Intelligence for Informatics]. Computing and Technologies (3ICT), pp. 239-244, doi: 10.1109/3ICT56508.2022.9990859.
5. Tang, Zh., Cui, J., Zhong, H., Yu, M., (2016). A Random PRESENT Encryption Algorithm Based on Dynamic S-box International. Journal of Security and Its Applications, 10(3), 383-392 http://dx.doi.org/10.14257/ijsia.2016.10.3.33
6. Shirai, T., Shibutani, T., Akishita, K., et al.(2007). The 128-bit blockcipher CLEFIA. FSE 2007. LNCS. – Vol. 4593, 181-195.
7. Kerry, A.M., Larry, B., Meltem, S.T., Nicky, M.(2017). Report on Lightweight Cryptography. https://doi.org/10.6028/NIST.IR.8114
8. NIST, (2018). Submission Requirements and Evaluation Criteria for the Lightweight Cryptography Standardization Process. https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/final-lwc-submission-requirements-august2018.pdf
9. Ishhukova, E.A., Tolomanenko, E.A. (2019) Analiz algoritmov shifrovanija maloresursnoj kriptografii v kontekste interneta veshhej. Sovremennye naukoemkie tehnologii, 3(2), 182-186. shttps://top-technologies.ru/ru/article/view?id=37462
10. Ischukova, E.A., Tolomanenko, E.A. (2019). Analysis of the algorithms for encryption of lightweight cryptography in the context of the Internet of Things [Modern High Technologies], No. 3-2. – Pp. 182-186, URL: https://top-technologies.ru/ru/article/view?id=37462
11. Babenko, L.K., Golotin, D.V., Makarevich, O.B. (2016). Sozdanie i issledovanie maloresursnoj realizacii potochnogo shifra Trivium. Izvestija JuFU, № 12, 42-54.
12. Alghamdi, Y., Munir, A. An Image Encryption Algorithm Based on Trivium Cipher and Random Substitution. SN COMPUT. SCI. 4, 713 (2023). https://doi.org/10.1007/s42979-023-02172-7
13. Suhail, A., Mir, N., Mehvish, A., Ishfaq, S., Tariq, B. M. (2022). FPGA Implementation of PRESENT Block Cypher with Optimised Substitution Box [2022 Smart Technologies], Communication and Robotics (STCR), pp.1-6. doi: 10.1109/STCR55312.2022.10009366.
14. Babenko, L.K., Bespalov, D.A., Makarevich, O.B., Chesnokov, R.D., Trubnikov, Ja.A. (2014). Razrabotka i issledovanie programmno-apparatnogo kompleksa shifrovanija po algoritmu Present dlja reshenija zadach maloresursnoj kriptografii. Izvestija JuFU. – № 2, 174-180.
15. Zhukov, A.E. (2015). Legkovesnaja kriptografija. Chast' 1. Voprosy kiberbezopasnosti, № 1, 26-43.
16. Barański, R., Galewski, M., Nitkiewicz, S. (2019). The study of Arduino Uno feasibility for DAQ purposes. Diagnostyka, 20(2), 33-48. https://doi.org/10.29354/diag/109174
17. Дюсенбаев Д.С., Алғазы К.Т., Сақан Қ.С. Симметриялы шифрларда қолданылатын сызықты емес түйіндерді зерттеу // Материалы международной научно-практической конференции «Актуальные проблемы информационной безопасности в Казахстане». – Алматы. 11 июня 2021 г. – С. 34-38.
18. Сейткулов Е., Оспанов Р., Ергалиева Б. О криптографических свойствах S-блоков // Вестник КазНИТУ, 2021, №143(4). – С.96-103 // https://doi.org/10.51301/vest.su.2021.i4.12.
19. Ibrahim, N. and Agbinya, J. (2022) A Review of Lightweight Cryptographic Schemes and Fundamental Cryptographic Characteristics of Boolean Functions. Advances in Internet of Things, 12, 9-17. doi: 10.4236/ait.2022.121002.

References

1. El-hajj M, Mousawi H, Fadlallah A. Analysis of Lightweight Cryptographic Algorithms on IoT Hardware Platform. Future Internet. 2023; 15(2):54. https://doi.org/10.3390/fi15020054
2. Podimatas P, Limniotis K. Evaluating the Performance of Lightweight Ciphers in Constrained Environments – The Case of Saturnin. Signals. 2022; 3(1):86-94. https://doi.org/10.3390/signals3010007
3. Hanacek, N. (2023). NIST Selects 'Lightweight Cryptography' Algorithms to Protect Small Devices. https://www.nist.gov/news-events/news/2023/02/nist-selects-lightweight-cryptography-algorithms-protect-small-devices
4. Hasan, H., Ali, G., Elmedany, W., Balakrishna C. (2022) Lightweight Encryption Algorithms for Internet of Things: A Review on Security and Performance Aspects [International Conference on Innovation and Intelligence for Informatics]. Computing and Technologies (3ICT), pp. 239-244, doi: 10.1109/3ICT56508.2022.9990859.
5. Tang, Zh., Cui, J., Zhong, H., Yu, M., (2016). A Random PRESENT Encryption Algorithm Based on Dynamic S-box International. Journal of Security and Its Applications, 10(3), 383-392 http://dx.doi.org/10.14257/ijsia.2016.10.3.33
6. Shirai, T., Shibutani, T., Akishita, K., et al.(2007). The 128-bit blockcipher CLEFIA. FSE 2007. LNCS, vol. 4593. – 181-195.
7. Kerry, A.M., Larry, B., Meltem, S.T., Nicky, M.(2017). Report on Lightweight Cryptography. https://doi.org/10.6028/NIST.IR.8114
8. NIST, (2018). Submission Requirements and Evaluation Criteria for the Lightweight Cryptography Standardization Process. https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/final-lwc-submission-requirements-august2018.pdf
9. Ishhukova, E.A., Tolomanenko, E.A. (2019) Analiz algoritmov shifrovanija maloresursnoj kriptografii v kontekste interneta veshhej. Sovremennye naukoemkie tehnologii, 3(2), 182-186. shttps://top-technologies.ru/ru/article/view?id=37462
10. Ischukova, E.A., Tolomanenko, E.A. (2019). Analysis of the algorithms for encryption of lightweight cryptography in the context of the Internet of Things [Modern High Technologies], No. 3-2, pp. 182-186, URL: https://top-technologies.ru/ru/article/view?id=37462
11. Babenko, L.K., Golotin, D.V., Makarevich, O.B. (2016). Sozdanie i issledovanie maloresursnoj realizacii potochnogo shifra Trivium. Izvestija JuFU, № 12, 42–54.
12. Alghamdi, Y., Munir, A. An Image Encryption Algorithm Based on Trivium Cipher and Random Substitution. SN COMPUT. SCI. 4, 713 (2023). https://doi.org/10.1007/s42979-023-02172-7
13. Suhail, A., Mir, N., Mehvish, A., Ishfaq, S., Tariq, B. M. (2022). FPGA Implementation of PRESENT Block Cypher with Optimised Substitution Box [2022 Smart Technologies], Communication and Robotics (STCR), pp.1-6. doi: 10.1109/STCR55312.2022.10009366.
14. Babenko, L.K., Bespalov, D.A., Makarevich, O.B., Chesnokov, R.D., Trubnikov, Ja.A. (2014). Razrabotka i issledovanie programmno-apparatnogo kompleksa shifrovanija po algoritmu Present dlja reshenija zadach maloresursnoj kriptografii. Izvestija JuFU, № 2, 174–180.
15. Zhukov, A.E. (2015). Legkovesnaja kriptografija. Chast' 1. Voprosy kiberbezopasnosti, № 1, 26–43.
16. Barański, R., Galewski, M., Nitkiewicz, S. (2019). The study of Arduino Uno feasibility for DAQ purposes. Diagnostyka, 20(2), 33-48. https://doi.org/10.29354/diag/109174
17. D.S. Dyusenbaev, K.T. Alghazy, K.S. Sakan. Study of non-linear nodes used in symmetric ciphers // Materials of international scientific-practical conference "Actual problems of information security in Kazakhstan". - Almaty. June 11, 2021. – P. 34-38.
18. Seitkulov E., Ospanov R., Yergalieva B. On cryptographic properties of S-blocks // Vestnik KazNITU, 2021, №143(4), – C.96-103 // https://doi.org/10.51301/vest.su.2021.i4.12.((in Russian).)
19. Ibrahim, N. and Agbinya, J. (2022) A Review of Lightweight Cryptographic Schemes and Fundamental Cryptographic Characteristics of Boolean Functions. Advances in Internet of Things, 12, 9-17. doi: 10.4236/ait.2022.121002.