MUHAMMAD AL-XORAZMIY
NOMIDAGI TATU FARG'ONA FILIALI

FERGANA BRANCH OF TUIT
NAMED AFTER MUHAMMAD AL-KHORAZMI

"AL-FARG'ONIY AVLODLARI"

ELEKTRON ILMIY JURNALI | ELECTRONIC SCIENTIFIC JOURNAL

TA'LIMDAGI ILMIY, OMMABOP VA ILMIY TADQIQOT ISHLARI

4-SON 1(8)
2024-YIL

TATU, FARG'ONA
O'ZBEKISTON

ISSN 2181-4252

O‘ZBEKISTON RESPUBLIKASI RAQAMLI TEXNOLOGIYALAR VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI FARG‘ONA FILIALI

Muassis: Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg‘ona filiali.
Chop etish tili: O‘zbek, ingliz, rus.
Jurnal texnika fanlariga ixtisoslashgan bo‘lib, barcha shu sohadagi matematika, fizika, axborot texnologiyalari yo‘nalishida maqolalar chop etib boradi.

Учредитель: Ферганский филиал Ташкентского университета информационных технологий имени Мухаммада ал-Хоразми.
Язык издания: узбекский, английский, русский.
Журнал специализируется на технических науках и публикует статьи в области математики, физики и информационных технологий.

Founder: Fergana branch of the Tashkent University of Information Technologies named after Muhammad al-Khorazmi.
Language of publication: Uzbek, English, Russian.
The magazine specializes in technical sciences and publishes articles in the field of mathematics, physics, and information technology.

2024 yil, Tom 1, №4
Vol.1, Iss.4, 2024 y

ELEKTRON ILMIY JURNALI **ELECTRONIC SCIENTIFIC JOURNAL**

«Al-Farg‘oniy avlodlari» («The descendants of al-Fargani», «Potomki al-Fergani») O‘zbekiston Respublikasi Prezidenti administratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligida 2022-yil 21 dekabrda 054493-son bilan ro‘yxatdan o‘tgan.

Jurnal OAK Rayosatining 2023-yil 30 sentabrdagi 343-sonli qarori bilan Texnika fanlari yo‘nalishida milliy nashrlar ro‘yxatiga kiritilgan.

Tahririyat manzili:
151100, Farg‘ona sh.,
Aeroport ko‘chasi 17-uy,
202A-xona
Tel: (+99899) 998-01-42
e-mail: info@al-fargoniy.uz

FARG’ONA - 2024 YIL

Jurnal quyidagi bazalarda indekslanadi:

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

Rasulov Akbarali Maxamatovich, Ibroximov Nodirbek Ikromjonovich, To‘xtasinov Azamat G‘ofurovich, NOYOB MIS METALL KLASTERLARINING GEOMETRIK TUZILISHINI KOMPYUTER EKSPERIMENTI ORQALI TADQIQ ETISH	7-11
Далиев Бахтиёр Сирожиддинович, Решение уравнения Абеля методом оптимальных квадратурных формул	12-15
Saidov Mansurjon Inomjonovich, Tartiblangan statistikalarda baholarni topish usullari	16-21
Kayumov Ahror Muminjonovich, TRIKOTAJ TO‘QIMASI TARKIBIDAGI IP XUSUSIYATLARI VA DEFORMATSIYAGA TA’SIRI	22-27
Muradov Farrux Abdukaxarovich, Kucharov Olimjon Ruzimurotovich, Narzullayeva Nigora Ulugbekovna, Eshboyeva Nodira Faxriddinovna, GAZLI ARALASHMALAR VA ZARARLI MODDALARNING ATMOSFERADA TARQALISHI MASALASINI YUQORI TARTIBLI APPROKSIMATSIYANI QO‘LLAGAN HOLDA UNI SONLI YECHISH ALGORITMI	28-37
Maniyozov Oybek Azatboyevich, NAVIER-STOKES TENGLAMASINI KLASSSIK HAMDA KLASSIK BO‘LMAGAN YECHIMLARINI VA UNING O`ZIGA XOSLIGI	38-44
Tillavoldiyev Azizbek Otabek o‘g‘li, Tibbiy tasvirlarda reprezentativ psevdoobyektlarni segmentatsiyalash algoritmi	45-51
Fayziev Shavkat Ismatovich, Karimov Sherzod Sobirjonovich, Muxtarov Alisher Muxtorovich, DDoS hujumlarni aniqlashda neyron tarmoqlarga asoslangan gibrid modellarni ishlab chiqish	52-58
Rasulmuxamedov Maxamadaziz Maxamadaminovich, Shukurova Shohsanam Bahriddin qizi, Mirzaeva Zamira Maxamadazizovna, MURAKKAB SHAKLLI, HAJMLI JISMLARNING ELASTOPLASTIK DEFORMATSIYASINING MATEMATIK MODELLARINI QURISH	59-63
Uzakov B.M., Melikuziyev M.R., TARELKALI TURDAGI REKTIFIKATSIYA KOLONNANING HARORAT KO‘RSATKICHLARINI MOSLASHUVCHAN BOSHQARISH	64-72
Порубай Оксана Витальевна, Эволюционные алгоритмы в задачах оптимизации режимов работы региональных энергосистем	73-77
Musayev Xurshid Sharifjonovich, TRIKOTAJ TO‘QIMA TASVIRLARINI ANIQLASH VA RAQAMLI ISHLOV BERISH USULLARI	78-81
Нурдинова Разияхон Абдихаликовна, ПОЛУПРОВОДНИКИ КАК МАТЕРИАЛЫ ДЛЯ ИЗГОТОВЛЕНИЯ ТЕРМОГЕНЕРАТОРОВ В МЕДИЦИНЕ	82-85
Мовлонов Пахловон Ибрагимович, ДЕГРАДАЦИЯ СЭ ПОД ДЕЙСТВИЕМ ИЗЛУЧЕНИЯ ВИДИМОЙ ОБЛАСТИ СПЕКТРА И ИОНИЗИРУЮЩЕЙ РАДИАЦИИ	86-90
Севинов Жасур Усманович, Темербекова Барнохон Маратовна, Маманазаров Улугбек Бахтиёр угли, Бекимбетов Баходир Маратович, Синтез методов цифровой регистрации в системах сбора и обработки измерительной информации для обеспечения достоверности в информационно-управляющих системах	91-96
O.S.Rayimdjonova, ISSIQLIK VA OPTOELEKTRON O‘ZGARTIRGICHLARNING ASOSIY TAVSIFLARI VA UMUMIY MASALALARI	97-100
Muradov Farrux Abdukaxarovich, Narzullayeva Nigora Ulugbekovna, Kucharov Olimjon Ruzimurotovich, Eshboyeva Nodira Faxriddinovna, ATMOSFERANING CHEGARAVIY QATLAMIDA GAZLI ARALASHMALAR VA ZARARLI MODDALARNING TARQALISHI MASALASINI O‘ZGARUVCHILARNI ALMASHTIRISH USULI YORDAMIDA IFODALASH VA UNING SONLI YECHISH ALGORITMI	101-107
Акбаров Давлатали Егиталиевич, Акбаров Умматали Йигиталиевич, Кучкоров Мавзуржон Хурсанбоевич, Умаров Шухратжон Азизжонович, РАЗРАБОТКА АЛГОРИТМА СИММЕТРИЧНОГО БЛОЧНОГО ШИФРОВАНИЯ НА ОСНОВЕ СЕТИ ФЕЙСТЕЛЯ ПО КРИПТОСТОЙКИМИ БАЗОВЫМИ ТАБЛИЧНЫМ ПРЕОБРАЗОВАНИЯМИ	108-113
Xolmatov Abrorjon Alisher o‘g‘li, Xoshimov Baxodirjon Muminjonovich, MAZUTNI REKTIFIKATSIYALASH QURILMALARINING VAKUUM YARATISH TIZIMINI TAKOMILLASHTIRISH	114-125
Goipova Xumora Qobiljon qizi, Dasturiy ta’minotdagi xatolarni avtomatik topish va tuzatish uchun o‘qitiladigan algoritmlar	126-129
Xudoykulov Z.T., Xudoynazarov U.U., YETARLI GOMOMORFIK SHIFRLASH ALGORITMLARI YORDAMIDA AXBOROTNI KRIPTOGRAFIK HIMOYALASH	130-135
Калашников Виталий Алексеевич, ОБОСНОВАНИЕ НЕОБХОДИМОСТИ СОЗДАНИЯ СПЕЦИАЛЬНОГО АГРЕГАТА ДЛЯ ПОСЕВА СЕМЯН ПШЕНИЦЫ В МЕЖДУРЯДЬЯ ХЛОПЧАТНИКА И ОПРЕДЕЛЕНИЕ ОСНОВНЫХ ПАРАМЕТРОВ ШАРНИРНО-ПОЛОЗОВИДНОГО СОШНИКА	136-143
Ermatova Zarina Qaxramonovna, To‘qimachilik sanoatida Linter qurilmalarining ahamiyatini o‘rganish va kuzatish	144-146
Tolipov Nodirjon Isaqovich, Madibragimova Iroda Mukhamedovna, ON A NON-CORRECT PROBLEM FOR A BIHARMONIC EQUATION IN A SEMICIRCLE	147-151
Xudoykulov Zarif Turakulovich, Qozoqova To‘xtajon Qaxramon qizi, PRESENT YENGIL VAZNLI KRIPTOGRAFIK ALGORITMINING TAHLILI	152-157
D.S.Yaxshibayev, A.H.Usmonov, Yer osti sizot suvlari sathi o‘zgarishini matematik modellashtirish va sonli tadbiq qilish	158-162

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

Tojimatov Dostonbek Xomidjon o‘g‘li, KIBERRAZVEDKA AMALIYOTIDA IOC, LOG VA DARK WEB MONITORING MA’LUMOTLARINING INTELLEKTUAL INTEGRATSIYASIGA ASOSLANGAN KIBERTAHDIDLARNI ERTA ANIQLASH MODELI	163-167
Mirzayev Jamshid Boymurodovich, MATNLI MA’LUMOTLARNI YASHIRIN UZATISHDA STEGANOGRAFIK USULLARDAN FOYDALANISH	168-172
Kabildjanov Aleksandr Sabitovich, Pulatov G‘iyos Gofurjonovich, Pulatova Gulxayo Azamjon qizi, LSTM MODELI ASOSIDA OB-HAVO SHAROITLARINING YURAK-QON BOSIMI KASALLIKLARIGA TA’SIRINI BASHORATLASH	173-177
Erejepov Keulimjay Kaymatdinovich, SHAXSNI OVOZI ORQALI IDENTIFIKATSIYALASH ALGORITMLARI	178-183
Muxtarov Ya., Obilov H., OPERATOR USULI YORDAMIDA O‘ZGARMAS KOEFFITSIENTLI CHIZIQLI DIFFERENSIAL TENGLAMALAR SISTEMASINI INTEGRALLASH	184-188
Tillaboev Muxiddinjon, PILLANI NAMLIGINI O‘LCHISHNING OPTOELEKTRON QURILMASI	189-192
Atajonova Saidakhon Boratalievna, Khasanova Makhinur Yuldashbayevna, INTEGRATION OF HYBRID SYSTEM ANALYSIS METHODS TO IMPROVE DECISION-MAKING EFFICIENCY	193-196
Зулунов Равшанбек Маматович, ТЕХНОЛОГИИ ROBOTIC PROCESS AUTOMATION В МЕДИЦИНЕ	197-200
Aliyev Ibratjon Xatamovich, Bilolov Inomjon Uktamovich, CREATING A MODEL OF THE FALL OF SOLAR ENERGY IN CERTAIN COORDINATES	201-204
Akbarov Xatam Ulmasaliyevich, Ergashev Dilshodbek Mamasidiqovich, RDB TOKARLIK DASTGOHIDA ISHLOV BERISH JARAYONINING MATEMATIK MODELINI YARATISH	205-209
Абдуллаев Темурбек Маруфжонович, Козлов Александр Павлович, Разработка интеллектуальной системы управления освещением на основе IoT - технологий	210-219
O‘rinboyev Johongir Kalbay o‘g‘li, Nugmanova Mavluda Avaz qizi, KLASTERLASH USULLARI YORDAMIDA NUTQNI AVTOMATIK SEGMENTATSIYALASH	220-225
Dalibekov Lochinbek Rustambekovich, 5G TARMOQLARIDA MASSIVE MIMO TEXNOLOGIYASINI JORIY ETISHNING TAHLILI	226-232
Bozarov Baxromjon Ilxomovich, Fure almashtirishlarini taqribiy hisoblash uchun optimal kvadratur formulalar	233-235
Xusanova Moxira Qurbonaliyevna, TARMOQ QURILMALARIDA DEMILITARIZATSIYALANGAN ZONA (DMZ) NI SOZLASH ORQALI XAVFSIZLIKNI TA’MINLASH	236-239
Ravshan Indiaminov, Sulton Khakberdiyev, INTERACTION BETWEEN MAGNETIC FIELDS AND THIN SHELLS	240-244
Muradov Muhammad Murod o‘g‘li, Mobil aloqa tayanch stansiyalarini qayta tiklanuvchan energiya ta’minot manbalaridan foydalangan holda energiya bilan ta’minlash xususiyatlari	245-250
Kabildjanov Aleksandr Sabitovich, Pulatov G‘iyos Gofurjonovich, Pulatova Gulxayo Azamjon qizi, OB-HAVO SHAROITLARINING YURAK QON BOSIMI KASALLIKLARIGA TA’SIRINI MLP MODELIDA OPTIMALLASHTIRISH	251-255
Okhunov Dilshod Mamatjonovich, Okhunov Mamatjon Xamidovich, Azizov IskandarAbdusalim ugli, Ismoilzhonov Abdullokh Farrukhbek ugli, THE USE OF BIG DATA IN THE DIGITAL ECONOMY	256-260
Abduraimov Dostonbek Egamnazar o‘g‘li, ELASTIKLIK NAZARIYASI MASALASIGA LIBMAN TIPIDAGI ITERATSION USULNI QO‘LLASHNING MATEMATIK MODELI	261-266
Мамадалиев Фозилжон Абдуллаевич, Новый подход составления математической модели для определения параметров торможения автомобиля в экстремальных условиях эксплуатаций	267-269
Nasriddinov Otadavlat Usubjonovich, FIZIK MASALALARNI MATEMATIK PAKETLAR YORDAMIDA MODELLASHTIRISH	270-272
Jo‘rayev Mansurbek Mirkomilovich, Ro’zaliyev Abdumalikjon Vahobjon o’g’li, AVTOMATLASHTIRILGAN MONITORING TIZIMI SIMSIZ SENSOR TARMOG‘IDA MA’LUMOTLARNI UZATISH	273-278
Shamsiyeva Xabiba Gafurovna, VIDEO MA’LUMOTLARGA ISHLOV BERISH VA KOMPYUTERLI KO’RISH ALGORITMLARINING APPARAT DASTURIY MAJMUI	279-284
Atajonov Muhiddin Odiljonovich, AVTONOM FOTOELEKTRIK MODULNI MODELLASHTIRISH	285-288
J.M. Kurbanov, S.S.Sabirov, J.J.Kurbonov, NANOKATALIZATOR OLISH TEXNOLOGIYASIDA “NAVBAHOR” BENTONITINI QURITISH VA KUYDIRISH JARAYONLARINING TERMOGRAVIMETRIK TAHLILI	289-293
Umarov Shukhratjon, Rakhmonov Ozodbek, ASSESSMENT OF THE LEVEL OF SECURITY AVAILABLE IN 4G AND 5G MOBILE COMMUNICATION NETWORKS	294-297
Soliyev Bahromjon Nabijonovich, Elektron tijorat savdolarini dasturiy yondashuvi tahlilida metodlar, matematik model va amaliy ko‘rsatkichlar	298-302
Asrayev Muhammadmullo Abdullajon o‘g‘li, SINFLAR ORASIDAGI MASOFA, QAROR QABUL QILISH QOIDASI VA AJRATISH FUNKSIYASI	303-305

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

Polvonov Baxtiyor Zaylobidinovich, Khudoyberdieva Muxayyoxon Zoirjon qizi, Abdubannabov Mo‘ydinjon Iqboljon o‘g‘li, Ergasheva Gulruxsor Qobiljon qizi, Tohirjonova Zahro Shovkatjon qizi, Mamasodiqov Shohjahon, CHARACTERIZATION OF PHOTOLUMINESCENCE SPECTRUM OF CHALCOGENIDE CADMIUM-BASED SEMICONDUCTOR POLYCRYSTALLINE FILMS	306-315
Sharibayev Nosirjon Yusupjanovich, Musayev Xurshid Sharifjonovich, TRIKOTAJ TO‘QIMALARINI REAL VAQT REJIMIDA ANIQLANGAN NUQSONLARNI TAHLIL QILISH	316-320
Эргашев Отабек Мирзапулатович, Асомиддинов Бекзод, СОЗДАНИЕ ПРОГРАММНЫХ МОДУЛЕЙ ДЛЯ РЕШЕНИЯ ФУНКЦИОНАЛЬНЫХ ЗАДАЧ ИНФОРМАЦИОННЫХ СИСТЕМ	321-326
Djurayev Sherzod Sobirjonovich, Ermatova Zarina Qaxramonovna, YANGI KONSTRUKSIYADAGI MULTISIKLON QURILMASINING ENERGIYA SAMARADORLIGINI TAHLIL QILISH	327-331
J.M. Kurbanov, S.S.Sabirov, J.J.Kurbonov, ”NAVBAHOR” BENTONITINING MODIFIKATSIYALANGAN NAMUNASINI O‘YUCH EMMda QIZDIRISH HARORATIGA QARAB TEKSTURA XUSUSIYATLARINING O‘ZGARISHI	332-337
Sharibayev Nosirjon Yusubjanovich, Kayumov Ahror Muminjonovich, SINOV YORDAMIDA TRIKOTAJ MAXSULOTLARINI SHAKL SAQLASH VA DEFORMATSIYALANISH JARAYONLARINI MONITORINGI	338-343
Muminov Kamolkhon Ziyodjon o’g’li, Artificial Intelligence in Cybersecurity, Revolutionizing Threat Detection and Response Systems	344-347
Тажибаев Илхом Бахтиёрович, ОБРАБОТКА МНОГОКАНАЛЬНЫХ СИГНАЛОВ В РАДИОЧАСТОТНЫХ И ОПТИЧЕСКИХ СИСТЕМАХ	348-351
Karimov Sardor Ilhom ugli, Sotvoldiyeva Dildora Botirjon qizi, Karimova Barnokhon Ibrahimjon qizi, COMPARISON OF MULTISERVICE REMOTE SENSING DATA FOR VEGETATION INDEX ANALYSIS	352-354
Abdurasulova Dilnoza Botirali kizi, PNEUMATIC AND HYDRAULIC TECHNICAL TOOLS OF AUTOMATION	355-359
Абдукадиров Бахтиёр Абдувахитович, СПОСОБЫ НАСТРОЙКИ ВЕСОВ ДЛЯ СНИЖЕНИЯ ПОТЕРЬ ПРИ ОБУЧЕНИИ ДАННЫХ В НЕЙРОННЫХ СЕТЯХ	360-365
Turakulov Otabek Xolmirzayevich, Mamaraufov Odil Abdixamitovich, IJTIMOIY TARMOQLARDA ELEKTRON MATNLI MA’LUMOTLARNI TASNIFLASHNING NEYRON-NORAVSHAN ALGORITMI	366-370
Asrayev Muhammadmullo Abdullajon og‘li, Muxtoriddinov Muhammadyusuf Temirxon o‘g‘li, REGIONS APPLICATIONS SYSTEMS RECOGNITION	371-373
Raximov Baxtiyor Nematovich, Yo‘ldosheva Dilfuza Shokir qizi, Majmuaviy markazlashtirilgan tizimlarning arxitekturasi va funksiyalari	374-378
Нурилло Мамадалиев Азизиллоевич, Моделирование конфликтных ситуаций телевизионных изображений в процессе обработки видеоинформации	379-381
А.А. Отахонов, ОБНАРУЖЕНИЕ И ОЦЕНКА ФИШИНГОВЫХ URL-АДРЕСОВ С ИСПОЛЬЗОВАНИЕМ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ	382-390
Akbarov Xatam Ulmasaliyevich, Ergashev Dilshodbek Mamasidiqovich, X12M MARKALI PO‘LAT UCHUN TERMOSIKLLI ISHLOV BERISHNI AMALGA OSHIRISH PARAMETRLARI	391-396
Abdukodirov Abduvaxit Gapirovich, Abdukadirov Baxtiyor Abduvaxitovich, YUZ TASVIRLARINI GEOMETRIK NORMALLASHTIRISH ALGORITMINI ISHLAB CHIQISH	397-401
D.B.Abdurasulova, T.U.Abduhafizov, RAQAMLI IQTISODIYOTNING O‘SISHI VA UNING TADBIRKORLIK FAOLIYATIGA TA’SIRI	402-405
Ibragimov Navro‘zbek Kimsanbayevich, Hududiy oliy ta’lim muassasalarida raqobat ustunligini ta’minlashning diagnostik tahlil qilish uchun dasturiy ta’minot	406-413
Melikuziyev Azimjon Latifjon ugli, USING COMPUTER-SIMULATOR PROGRAMS IN TEACHING PARALINGUISTIC UNITS	414-417
Soliyev B.N., Ismoilova M.R., ELEKTRON TIJORATDA QAYTARILISHLARNI OPTIMALLASHTIRISH VA ULARNING NATIJALARI	418-421
Ergashev Otabek Mirzapulatovich, FUZZY RULE BASE DESIGN FOR NUMERICAL DATA ANALYSIS	422-428
Abdukadirova Gulbahor Xomidjon qizi, Abduqodirova Mohizoda Ilxomidin qizi, YUZ TASVIRLARIGA DASTLABKI ISHLOV BERISHDA NEYRON TARMOQ ALGORITMLARINI QO‘LLASH SAMARADORLIGI	429-436
Садикова Мунира Алишеровна, ТРАНСФОРМАЦИЯ УПРАВЛЕНИЯ В ЦИФРОВУЮ ЭПОХУ	437-444
Pulatov Sherzod Utkurovich, Djumaniyazov Otabek Baxtiyarovich, THE ROLE OF IoT TECHNOLOGIES IN MONITORING THE ENVIRONMENTAL IMPACT OF INDUSTRIAL ENTERPRISES IN THE KHOREZM REGION	445-448
Mukhammadyunus Norinov, RESEARCH ON INCREASING THE BRIGHTNESS OF TELEVISION IMAGES	449-455
Arabboyev Alisher Avazbek o‘g‘li, DIFFIE-HELLMAN ALGORITMI VA XAVFSIZ KALIT ALMASHISH PROTOKOLLARI	456-458
Raximov Baxtiyor Nematovich, G‘oipova Xumora Qobiljon qizi, Ovoz tovushlari intelektual taxlili asosida videokuzatuz tizimini boshqarish	459-462

РАЗРАБОТКА АЛГОРИТМА СИММЕТРИЧНОГО БЛОЧНОГО ШИФРОВАНИЯ НА ОСНОВЕ СЕТИ ФЕЙСТЕЛЯ ПО КРИПТОСТОЙКИМИ БАЗОВЫМИ ТАБЛИЧНЫМ ПРЕОБРАЗОВАНИЯМИ

Акбаров Давлатали Егиталиевич,
Профессор кафедры математики Кокандский государственный педагогический института

Акбаров Умматали Йигиталиевич,
Доцент кафедры математики Кокандский государственный педагогический института

Кучкоров Мавзуржон Хурсанбоевич,
Доцент кафедры физика и астраномия Кокандский государственный педагогический института

Умаров Шухратжон Азизжонович,
Доцент кафедры информационной безопасности Ферганского филиала ТУИТ

Аннотация. В стати рассматриваются вопросы исследование и создание симметричного блочного алгоритма шифрования на основе сети Фейстеля по криптостойкими табличными базовыми преобразованиями. Такие алгоритмы блочного шифрования являются эффективными по разработке программных и аппаратных средств сети информационной коммуникации.

Ключевая слова: шифрования; алгоритм; сети Фейстеля; табличной замены; стойкость алгоритма; конкитинация; раунд ключ

ВВЕДЕНИЕ

В предлагаемой статье рассматриваются вопросы исследование и создание симметричного блочного алгоритма шифрования на основе сети Фейстеля по криптостойкими табличными базовыми преобразованиями. Список источников посвященные на тему сети Фейстеля, об их криптографических особенностях, свойствах, разработках разными новыми базовыми преобразованиями, приложениях и других назначениях в сети информационной коммуникации широко [1-9, и др.].

МАТЕРИАЛЫ И МЕТОДЫ

Аппаратные реализации базовых табличных преобразований алгоритмов являются удобными и рациональными, так как они не требуют вычисления, требуют только сравнения и переходы в перемешивании и распртострании битов или их объединения, при этом обеспечивая криптографической стойкости отображений.

Работа [10] посвящается исследованию вопросы криптографической стойкости таблиц логических операций и других табличных преобразований с объединениями битов. Установлены необходимые и достаточные условия стойкости табличных преобразований.

В предлагаемой статье исследуются вопросы стойкого блочного алгоритма шифрования по сети Фейстеля с базовыми преобразованиями таблиц логических операций и таблиц объединениями битов.

Результаты и обсуждение

Отмечается, что сети Фейстеля шифрования данных осуществляет под блоками битов шифруемого текста с ключами раундов. Ключи раундов имеют 32 битов, они образуются из

исходного ключа длина, которой не меньше 256 битов. Перед шифрованием открытого текста его разделяют под блоки 32 битов. При этом, если длина шифруемого текста не является кратным на 32 битов, то он добавляется до кратного с пробелами. Ниже приводится блочная схема *i*-раунда для алгоритма шифрования с битами, где базовыми преобразованиями являются: конкитинация (соединение) шифруемого 32-битного блока с ключом раунда, 32-битного блока, преобразование побитной табличной замены с таблицей истинности логических операций, циклический сдвиг на 11 битов (Рис 1).

1. Конкитинация (соединение) блоков соответствующей шифруемой части на *i*-ом раунде открытого текста $x_1(i)x_2(i)...x_{31}(i)x_{32}(i)k_{32}(i)$ с ключом раунда $k_1(i)k_2(i)....k_{31}(i)k_{32}(i)$ осуществляется следующим образом: $x_1(i)k_1(i)x_2(i)k_2(i)...x_{31}(i)k_{31}(i)x_{32}(i)k_{32}(i)$.

2. Осуществляется преобразование побитной табличной замены шифр величину шифруемого открытого сообщения на шифр обозначение с таблицей истинности логических операций: по пересечению столбца $x_j(i),\ j=1,2,...,32;$ и строку $k_t(i),\ t=1,2,...,32.$; находится шифр обозначение. То есть по входам $x_j(i)k_t(i).$ и $k_t(i).$, указанных, в алгоритме S_λ λ =1,..,32 блоков, определяются шифр обозначения.

3. Сдвиг циклический на 11 (или 7, 17,19) битов осуществляется присоединением контактов порядком: 12-бита с первым битом $a_1(i)$ левого 32-ух битного блока L_i (32 *bit*)=$a_1(i)a_2(i)…a_{32}(i)$, 13-бита с $a_2(i)$ и так далее, 32-бита с $a_{11}(i)$.

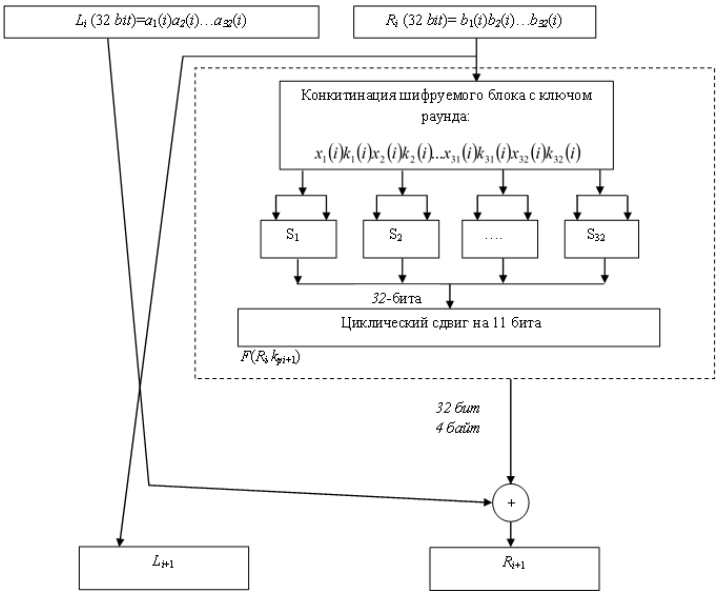

Рис 1. Блочная схема *i*-раунда для алгоритма шифрования с битами

Здесь стоит, отметит ещё следующие свойства сети Фейстеля. Математическая модель шифрования $i-$раунда выражается следующим образом:

$$\begin{cases} L_i = R_{i-1}, \\ R_i = L_{i-1} \oplus F(R_{i-1}, K_i). \end{cases}$$

Отсюда по свойству операции $\oplus$, математическая модель дешифрования $i-$раунда выражается:

$$\begin{cases} R_{i-1} = L_i, \\ L_{i-1} = R_i \oplus F(L_i, K_i). \end{cases}$$

Далее, рассматривается, когда шифрования осуществляется с парами битов, базовыми преобразованиями пару битов:

– конкитинация (соединение) шифруемого 32-битного блока с ключом раунда, выделенных, на 16 пары битов вида «00», «01», «10», «11»;

– осуществить преобразование 32-битных блоков, выделенных на 16 пары битов, табличной заменой с заданной табличной истинности с размером 4×4;

– циклический сдвиг на 11 битов.

1. Конкитинация (соединение) с парами битов блоков соответствующей шифруемой части на *i*-ом раунде открытого текста

$x_1(i)x_2(i)...x_{31}(i)x_{32}(i)k_{32}(i)$ с ключом раунда $k_1(i)k_2(i)....k_{31}(i)k_{32}(i)$ осуществляется следующим образом: $x_1(i)k_1(i)x_2(i)k_2(i)...x_{31}(i)k_{31}(i)x_{32}(i)k_{32}(i)$.

2. Осуществляется преобразование с парами битов табличной замены шифр величину шифруемого открытого сообщения на шифр обозначение с таблицей истинности размером 4×4: по пересечению столбца $x_j(i), x_{j+1}(i)\ \ j=1,2,...,31;$ и строку $k_t(i)k_{t+1}(i),\ \ t=1,2,...,31.$ находится шифр обозначение. То есть по входам $x_j(i)x_{j+1}(i).$ и $k_t(i)k_{t+1}(i).$, указанных, в алгоритме $S_\lambda\ \lambda$ =1,..,16 блоков, определяются шифр обозначения.

Здесь, например, приводится вид один из таблицы истинности размером 4×4:

k/x	00	01	10	11
00	10	11	00	01
01	11	00	01	10
10	00	01	10	11
11	01	10	11	00

Где значения: "00", "01", "10", "11", соответствующие на шифробозначениям, распределены равномерно, т.е. каждый из них повторяются 4 раза. Такое случае, обеспечит криптографической стойкости преобразования табличной замены [10].

3. Циклический сдвиг на 11 (или 7, 17,19) битов осуществляется присоединением контактов порядком: 12-бита с первым битом $a_1(i)$ левого 32-ух битного блока L_i (32 *bit*)=$a_1(i)a_2(i)…a_{32}(i)$, 13-бита с $a_2(i)$. далее, 32-ого бита с $a_{11}(i)$. Шифрование, с парами (четным числом) битов, а сдвиг на простое число больше чем 2 , положительно влияет на стойкость.

Ниже приводится блочная схема *i*-раунда для алгоритма шифрования с парами битов (рис 2).

Теперь, приводится общая блочная схема с совокупностью базовых преобразований $F(R_i k_{i+1})$ или $F(R_i K_{i+1})$: *конкитинация (соединение) битов или с парами битов, преобразование побитной табличной замены шифр величину шифруемого открытого сообщения на шифр обозначение с таблицей истинности логических операций или с парами битов, а сдвиг на простое число* положительно влияет на стойкость.

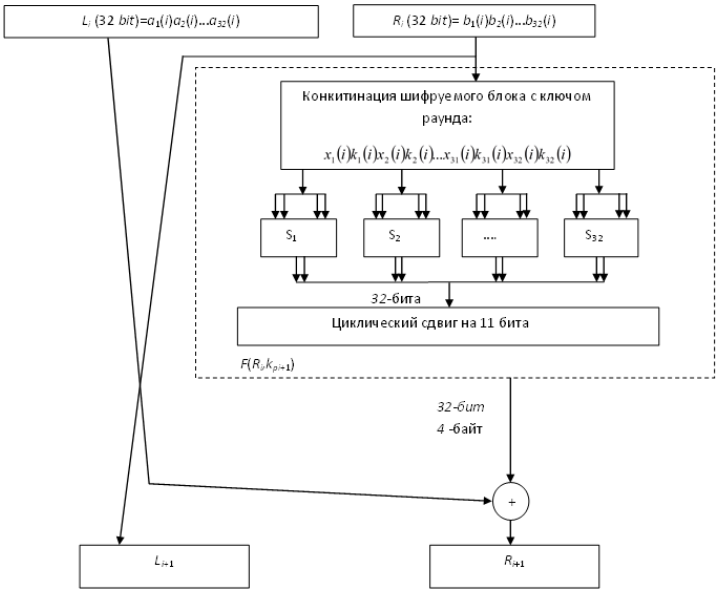

Рис 2. Блочная схема *i*-раунда для алгоритма шифрования с парами битов

В нижеприведенной общей блочной схеме алгоритма шифрования определены преобразования: $T_к=(R_8,L_8)$ -конечный блок шифрованного сообщения и побитное сложение этого блока с конечным ключом k_k, т.е. $T_ш=T_к\oplus k_k=(R_8,L_8)\oplus k_k$ (Рис 3). Такие определения преобразования конструкции алгоритмов с одной стороны повышает стойкость, с другой стороны обеспечить удобства в разработке эффективных конструкций программных и аппаратных средств на основе предложенных алгоритмов, базирующихся на сети Фейстеля. Действительно, в качестве входного блока принимая блок $T_ш$ в качестве начального

ключа k_k, применяя ключи раундов в обратном порядке: $k_н$, k_{p8}, …, k_{p1}, $k_н$ осуществляется процесс дешифрования блоков шифрованного сообщения [1-3] как шифрования.

С развитием вычислительных методов и технологии независимо криптографической стойкости преобразования, применяемые как стандарт алгоритмы шифрования гарантированной стойкости, теряются за счет малой длины ключа. По другому выражению стойкость алгоритма естественным образом ослабляется. Поэтому возникает задача: сохраняя базовых преобразований алгоритма, удлинять их исходные ключи и ключи раундов [3,7-10].

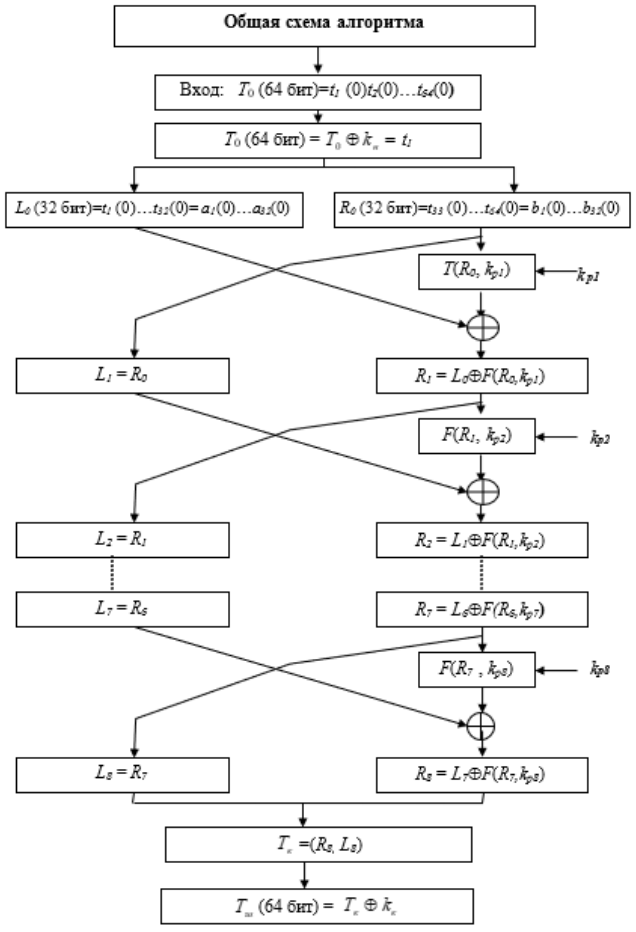

Рис 3. Общей блочной схеме алгоритма шифрования определены преобразования

Блочная схема решения такую задачу для алгоритмов, основанных на сети Фейстеля, может выглядеть следующем виде:

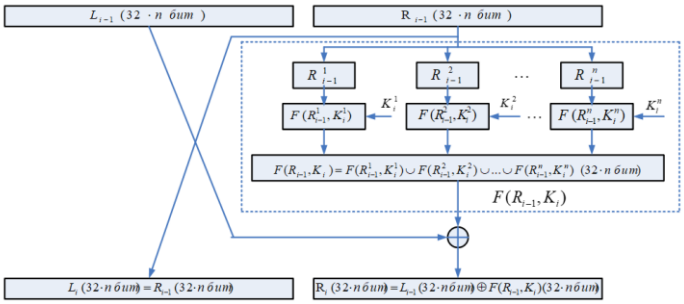

Рис 4. $i-$раунд модифицированной сети Фейстеля.

Где:

1. Длина блока $64m$ *бит*, $m = 1,2,\ldots \prec \infty$; открытого текста. Длина исходного ключа $|K| \cdot n$ *бит* $n = 2,\ldots \prec \infty$.
2. Объединение частей ключа $K_i = K_i^1 K_i^2 \ldots K_i^n - i$ -раунда.
3. Длины $R_i -$ левой и $L_i -$ правой частей сети Фейстеля: $|L| = |R| = 32 \cdot n$ *бит*.
4. $L_{i-1}(32 \cdot n$ *бит*$) -$ правая часть i-раунда.
5. $R_{i-1}(32 \cdot n$ *бит*$) -$ левая часть i-раунда.
6. $L^1_{i-1}(32$ *бит*$)$, $L^2_{i-1}(32$ *бит*$)$,..., $L^n_{i-1}(32$ *бит*$) -$ 32 *битные* частей ключа i-раунда.
7. $R^1_{i-1}(32$ *бит*$)$, $R^2_{i-1}(32$ *бит*$)$,..., $R^n_{i-1}(32$ *бит*$) - i$ -раунд, левой части.
8. $F(R^1_{i-1}, K^1_i)$, $F(R^2_{i-1}, K^2_i)$,..., $F(R^n_{i-1}, K^n_i) - i$ - раунд, соответствующие преобразования функции Фейстеля.

Математическая модель модифицированной сети Фейстел $i-$раунди имеет вид:

$$\begin{cases} L_i(32 \cdot n \ \textit{бит}) = R_{i-1}(32 \cdot n \ \textit{бит}) \\ R_i(32 \cdot n \ \textit{бит}) = L_{i-1}(32 \cdot n \ \textit{бит}) \oplus F(R_{i-1}, K_i)(32 \cdot \end{cases}$$

Из вышеприведённой модифицированной сети Фейстеля видно, что в зависимости значения n, присутствуют функции Фейстеля $F(R_{i-1}^1, K_i^1)$, $F(R_{i-1}^2, K_i^2)$,..., $F(R_{i-1}^n, K_i^n)$. Это позволяет использовать нескольких существующих алгоритмов с испытанными эффективными преобразованиями и S-блоков при увеличении длины ключа. Отмечается, что при $n=1$ длина ключа 256, $n=2$ длина ключа 512 и так далее. В общем виде приведенной модификации имеет место $l_1 = l \cdot n$, где $l-$является длина ключа основного модифицируемого алгоритма на основе сети Фейстеля.

Скорость шифрования/дешифрования основного и модифицированного алгоритмов одинаковы, так как количество осуществляемые преобразования одинаковы [3,4,6-8].

ЗАКЛЮЧЕНИЕ

Таким образом, предложенные модифицированные сети Фейстеля имеют следующие преимущества:

1. Сохраняя криптографической конструкции и свойства базовых преобразований, увеличит стойкость алгоритма за счет увеличения значения некоторых параметров алгоритма.

2. Сохраняя свойства и стойкость преобразований увеличить длину ключа алгоритма. Это обеспечить стойкость алгоритма относительно криптографической атаки полного перебора самому исходному ключу алгоритма и ключам раундов с базовыми преобразованиями.

3. Скорости исходного алгоритма и модифицированного одинаково. Такое обстоятельство обеспечить эффективность модификации относительно разработки программных и аппаратных средств алгоритма в приложения.

4. Предложенные алгоритмы с базовыми преобразованиями: *конкитинация* (*присоединение*) шифруемого блока открытого сообщения с ключом раунда, *табличная замена* шифр величину на шифр обозначения, циклический сдвиг на простое число больше чем 7, являются простыми процедурами не требующие вычислений. Такое обстоятельство позволяет желаемые возможности программной и аппаратной реализации таких алгоритмов. Учитывая важность и актуальность решения задачи было бы несообразным должное внимание, со стороны научными специалистами, на полученные и опубликованные результаты авторов.

ЛИТЕРАТУРА

1. Шнайер, Б. (2002). Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 816(3).

2. Алферов, А. П., Зубов, А. Ю., Кузьмин, А. С., & Черемушкин, А. В. (2001). Основы криптографии. М.: Гелиос арв, 200, 480.

3. Акбаров, Д. Е. (2009). Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши. Ўзбекистон маркаси, 432.

4. Akbarov, D., & Abdukadirov, A. (2022, June). Research of general mathematical characteristics of logical operations and table replacements in cryptographic transformations. In AIP Conference Proceedings (Vol. 2432, No. 1). AIP Publishing.

5. Зензин, О. С., & Иванов, М. А. (2002). Стандарт криптографической защиты XXI века–AES. Теория конечных полей/Под ред. МА Иванова. М.: КУДИЦ-ОБРАЗ, 2002.–340 с.

6. Akbarov, D. E., Kushmatov, O. E., Umarov, S. A., Bozarov, B. I., & Abduolimova, M. Q. (2021). Research on General Mathematical Characteristics of Boolean Functions’ Models and their Logical Operations and Table Replacement in Cryptographic Transformations. Central asian journal of mathematical theory and computer sciences, 2(11), 36-43.

7. Umarov, S. A., & Akbarov, D. E. (2016). Working out the new algorithm enciphered the data with a symmetric key. Journal of Siberian Federal University. Engineering & Technologies, 9(2), 214.

8. Bakhtiyor, A., & Shuxratjon, U. (2016). View of Models of Multiple Valuable Boolean Functions as Well as Implementation in Cryptographic Reflections. In Proceedings of International Conference on Application of Information and Communication Technology and Statistics in Economy and Education (ICAICTSEE) (pp. 91-95). International Conference on Application of Information and Communication Technology and Statistics and Economy and Education (ICAICTSEE).

9. Akbarov, D. E., & Umarov, S. A. (2016). Новый алгоритм блочного шифрования данных с симметричным ключом. Вісник Київського політехнічного інституту. Серія Приладобудування, (52 (2)), 82-91.

10. Акбаров, Д. Е., & Умаров, Ш. А. ДОСТАТОЧНОЕ УСЛОВИЕ НЕЛИНЕЙНОСТИ И БУЛЕВЫЕ ФУНКЦИИ ЛОГИЧЕСКИХ ТАБЛИЧНЫХ ПРЕОБРАЗОВАНИЙ. ЖУРНАЛИ, 19.

11. Фомичёв, В. (2023). Криптографические методы защиты информации. Курс лекций. Litres.