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

1-SON 1(5)
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, №1
Vol.1, Iss.1, 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:

Google Scholar · zenodo · ORCID · CYBERLENINKA · WORLD of JOURNALS · Directory of Research Journals Indexing

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

Mavjud oqimli shifrlash algoritmlarining qiyosiy tahlili

Xudoyqulov Zarifjon Turakulovich
texnika fanlari bo‘yicha falsafa doktori(PhD), dotsent
Muhammad al-Xorazmiy nomidagi
Toshkent axborot texnologiyalari universiteti,
Toshkent, O‘zbekiston

Rahmatullayev Ilhom Rahmatullayevich
texnika fanlari bo‘yicha falsafa doktori(PhD),
Muhammad al-Xorazmiy nomidagi
Toshkent axborot texnologiyalari universiteti Samarqand filiali
Samarqand, O‘zbekiston
Ilhom9001@gmail.com

Annotatsiya. Mazkur ishda yangi mavjud oqimli shifrlash algoritmlarini qiyosiy tahlil qilingan. Yangi mavjud oqimli shifrlash algoritmlarining qiyosiy tahlili, ularning xususiyatlari va parametrlarini o‘rganish orqali amalga oshiriladi. Tahlil qilingan algoritmlarning xossalari umumiy kriptografik talablar asosida umumlashtirilgan jadvali yaratilgan. Algoritmlarning xususiyatlari bo‘yicha olingan natijalar parametrlari solishtirilgan.

Kalit so‘zlar: Oqimli shifrlash, eSTREAM, Trivium, Rabbit, kriptotahlil, baholash, iteratsiya.

I. Kirish. Ana’naviy oqimli shifrlash algoritmlari va ularga aloqador xavfsizlik muammolari haqida ko'plab adabiyotlarda ma'lumot berilgan[1]. Ushbu algoritmlar o‘z vaqtida keng qo‘llanilgan bo‘lsada, ularning dizaynida yoki amalga oshirilishida aniqlangan xavfsizlik zaifliklari sababli, yangi ilovalar yoki tizimlarda ulardan foydalanish tavsiya etilmaydi. Bu zaifliklar, hujumchilarga ma’lumotlarni oshkor qilish, kalitlarni tiklash yoki shifrlangan ma’lumotlarni o‘zgartirish imkoniyatini beradi.

Quyida esa eSTREAM loyihasi doirasida ishlab chiqilgan ko‘plab oqimli shifrlash algoritmlarining tahlili bilan tanishib chiqiladi. eSTREAM loyihasi, European Network of Excellence for Cryptology II (ECRYPT II) doirasida ishga tushirilgan va oqimli shifrlash algoritmlariga bag‘ishlangan tashabbusdir[4]. Bu loyiha, mavjud oqimli shifrlash algoritmlarining xavfsizlik va samaradorlik jihatidan cheklovlarini engish maqsadida yangi, xavfsiz va samarali oqimli shifrlash algoritmlarini rivojlantirishni ko‘zlagan.

Ushbu loyihada ikki turdagi: dasturiy vositalar va qurilmalar uchun mos bo‘lgan oqimli shifrlash algoritmlari keltirilgan. Birinchi guruh algoritmlari dasturiy ko‘rinishda qulay bo‘lgan algoritmlardan iborat bo‘lib, 128-bitli AES-CTR algoritmidan tezkor bo‘lgan algoritmlardan tashkil topgan. Ushbu guruhga tegishli finalchi shifrlar: Salsa20/12, Rabbit, HC-128 va SOSEMANUK algoritmlaridan iborat. Ikkinchi guruhga tegishli shifrlar, eSTREAM loyihasi doirasida tanlangan, qurilmada amalga oshirish qulayligi nuqtai nazaridan 80-bitli AES algoritmidan ko‘ra afzalliklarga ega bo'lgan oqimli shifrlash algoritmlaridan iborat. Bu guruhda esa finalchi algoritmlar: Grain, Trivium [8] va MICKEY 2.0 iborat bo‘lgan.

II. Asosiy qism. eSTREAM loyihasi doirasida olib borilgan tanlov jarayonida, kriptografik hamjamiyatning diqqat markazida bo‘lgan bir qator muhim masalalar ko‘tarildi. Ushbu loyihada ishtirok etgan 34 ta shifrlash algoritmi orasidan, faqat ikkita sinxronlanuvchi shifrlar xavfsizlik muammolari sababli tanlovni tark etgan yoki tanlov jarayonida ularning xavfsiz emasligi aniqlangan. Bu holat, oqimli shifrlash algoritmlarining xavfsizlik darajasini baholashda qanday qat’iy mezonlar qo‘llanilishi kerakligini ko‘rsatadi.

Finalchi algoritmlar tanlovi, ularning kalitni to‘liq tanlash hujumiga qarshi samaradorligi kabi

muhim kriptografik xususiyatlarini sinovdan o‘tkazish orqali amalga oshirildi. Biroq, yangi kriptotahlil usullari qo‘llanilganda, finalchilar orasida jiddiy xavfsizlik muammolari aniqlandi. Bu, har qanday shifrlash algoritmi dizayni va tanlovi jarayonida, xavfsizlikni har tomonlama kafolatlash uchun keng qamrovli tahlil va sinovlarni o‘tkazish zarurligini ta’kidlaydi.

Lightweight Cryptography (LWC) muhiti, resurs cheklangan qurilmalar uchun mo‘ljallangan kriptografik algoritmlarni o‘z ichiga oladi. Bu turdagi muhitlar, masalan, IoT (Internet of Things) qurilmalari, o‘rnatilgan tizimlar, RFID teklar va smart kartalar kabi, cheklangan xotira, quvvat va protsessor quvvatiga ega bo‘lgan qurilmalardir. LWC muhitida samaradorlik, xavfsizlik va resurs talablarining muvozanati juda muhimdir. Shu munosabat bilan, eSTREAM loyihasining ikkinchi guruhiga tegishli Grain va Trivium algoritmlari hamda birinchi guruhga tegishli Salsa20 va Rabbit algoritmlari LWC muhitida qo‘llanish uchun mos keladi.

Adabiyotalar tahlili. *Dasturiy ko‘rinishda amalga oshirish uchun mos bo‘lgan shifrlar – birinchi guruh algoritmlari.* Salsa20 algoritmi, Daniel J. Bernstein tomonidan ishlab chiqilgan va eSTREAM loyihasining dasturiy ko‘rinishda amalga oshirish uchun mo‘ljallangan shifrlaridan biri sifatida tanlangan. Uning asosiy xususiyati, samaradorlik va xavfsizlik o‘rtasidagi muvozanatni ta'minlashdir. Salsa20, yuqori darajadagi parallel ishlash qobiliyati va sodda tuzilishi bilan ajralib turadi, bu esa uni turli platformalarda samarali ishlashga imkon beradi. 256 bitli kalit va 128 bitli IV (Initialization Vector) dan foydalanish, algoritmini keng ko‘lamli dasturlar uchun mos keladi. Salsa20 algoritmining uch varianti turli xil ilovalar va xavfsizlik hamda tezlik talablariga javob berish uchun mo‘ljallangan. Bu variantlar algoritmning raundlar soni bilan farqlanadi, bu esa ularning xavfsizlik darajasini va ishlov berish tezligini to'g'ridan-to'g'ri ta'sirlaydi. Salsa20/20 varianti odatdagi kriptografik ilovalar uchun mo‘ljallangan bo‘lsa, Salsa20/12 va Salsa20/8 variantlari yuqori tezlikni talab etuvchi, lekin, kam xavfsizlik darajasi mos keluvchi muhitlar uchun mos hisoblanadi. Salsa20 algoritmi, uning dasturiy ko‘rinishda amalga oshirilishi uchun juda qulay bo'lgan sodda, ammo samarali amallardan foydalanadi. Bu algoritm, ARX (Addition, Rotation, XOR) dizayn sxemasiga asoslanadi, bu sxema oddiy qo'shish, modul 2^{32} bo‘yicha qo‘shish, bitlar bo‘yicha siljitish (rotation) va XOR (eksklyuziv yoki) amallaridan iborat. (1-rasm). Ushbu algoritmda ma’lumotni shifrlash va deshifrlash bir xil bo‘lib, bu tezkorlikni ta’minlaydi. Ushbu algoritmlar tezkor algoritm bo‘lgani sababli, Crypto++ kriptografik kutubxonasidan joy olgan.

Salsa20 algoritmining dasturiy ko‘rinishi juda samarali bo‘lishi mumkin, masalan, eng optimal tarzda yozilganda 1452 bayt hajmga ega bo‘lib, shifrlash jarayoni uchun taxminan 18400 takt (sikl) talab qilishi bilan ajralib turadi. Bu, zamonaviy kompyuterlar va mikrokontrollerlar uchun juda samarali bo‘lgan tezlikni anglatadi, chunki u yuqori darajadagi optimallashtirish orqali amalga oshirilgan.

Biroq, algoritmining apparat ko‘rinishida amalga oshirilishi ancha ko‘p resurslarni talab qiladi. Masalan, eng optimal ravishda amalga oshirilgan apparat ko‘rinishi 12126 ta mantiqiy elementni (Gate Equivalent, GE) talab qiladi. Bu ko‘rsatkich, Lightweight Cryptography (LWC) uchun belgilangan standartlarga mos kelmaydi. LWC sohasida ko‘plab tadqiqotchilar apparat resurslarining juda cheklangan bo‘lishi kerakligini ta'kidlashadi, ba’zilar esa 300 GE atrofida bo‘lishini ideal deb hisoblashadi. Bu, asosan, juda kichik o‘lchamdagi qurilmalar uchun, masalan, RFID teklar yoki boshqa o‘rnatilgan tizimlar uchun juda muhimdir, chunki bu turdagi qurilmalar juda cheklangan xotira va ishlov berish quvvatiga ega.

Salsa20ning bu kabi apparat talablari, uni ba’zi LWC ilovalari uchun kamroq mos keladigan variantga aylantiradi, ayniqsa agar juda kichik o‘lchamdagi qurilmalar yoki juda cheklangan apparat resurslariga ega bo‘lgan muhitlar nazarda tutilsa. Shunga qaramay, Salsa20ning dasturiy ko‘rinishi, o‘rta va yuqori darajadagi qurilmalarda, shuningdek, kompyuter tarmoqlarida juda samarali va xavfsiz yechim bo‘lib qolmoqda.

Rabbit algoritmi, yuqori tezlik va samaradorlikka ega bo‘lgan sinxronlanuvchi oqimli

shifrlash algoritmidir. Bu algoritm, asosan, kalitni aralashtirish va ma’lumotlarni shifrlash jarayonlarini tezkor amalga oshirishga mo‘ljallangan bo‘lib, dasturiy vosita ko‘rinishida amalga oshirish uchun juda qulaydir. Rabbitning yuqori ishlov berish tezligi uni Internet protokollari, jumladan, video streaming, o‘yinlar va boshqa katta hajmdagi ma’lumotlarni yuborish talab etiladigan muhitlar uchun ideal tanlovga aylantiradi.Ushbu algoritm o‘rnatiluvchi tizimlar CyasSLdagi kriptografik algoritmlar ro‘yxatiga kiritilgan va ISO/IEC 18 033-4:2011 tarkibida standartlashtirilgan.

Ushbu algoritm zamonaviy protsessorlar uchun mos bo‘lgan sodda va asos amallardan tashkil topgan. Ushbu algoritm NFSR va S – jadvalga asoslanmagan kuchli chiziqsizlikni ta’minlaydi. Ushbu algoritmda nochiziqlik xaotik xarita asosida ta’minlangan. Rabbit algoritmi, yuqori tezlik va effektivlikka ega bo‘lgan sinxron oqimli shifrlash algoritmi sifatida, 128 bitlik kalit va 64 bitlik IV (Initialization Vector) dan foydalanadi. Bu xususiyatlar uni zamonaviy kriptografik talablarga javob beradigan qiladi. Ushbu algoritmni 1.7 Gs bo‘lgan Pentium 4 muhitida amalga oshirish uchun 1976 bayt talab etiladi va 486 sikl kalitni o‘rnatish va bir baytni shifrlash uchun 5.1 sikl talab qilinadi. Ushbu algoritm qurilmalar uchun mos bo‘lib, 3800 GE talab qiladi. Amaliy buzulishga olib keluvchi hujum (Practical fault) o‘rtacha 128-256 ta buzilishni talab qiladi va to‘liq ichki holatni tiklash uchun 241.6 baytli jadval talab qilinadi hamda bu 238 qadamni o‘z ichiga oladi.

HC shifrining ikki ko‘rinishi: HC-128 va HC-256 [9] mavjud bo‘lib, ular mos ravishda 128 va 256 bitli kalit va 128 bitli IV dan foydalanadilar. Ushbu shifr ikkita katta jadvaldan iborat bo‘lib, ularning har biri 32 bitli 512 ta elementdan iborat va 32 – bitli so‘zlar sifatida qaraladi. Har bir qadamda holat nochiziqli qayta aloqali funksiya yordamida yangilanadi va nochiziqli filtr funksiyadan 32 bitli natija chiqariladi. Ushbu algoritm parallel hisoblash muhiti va mikroprotsessorlar uchun mos hisoblanadi. Ushbu algoritm ham o‘rnatilgan tizimlar uchun foydalaniladigan CyasSL kriptografik kutubxonasida mavjud.

Ushbu algoritm jadvalga asoslangani bois, katta ma’lumotlarni shifrlash uchun dasturiy ko‘rinishda amalga oshirishga qulay. Biroq, ushbu algoritmni qurilmada amalga oshirish murakkab bo‘lib, 52 400 GE imkoniyatini talab etadi. Ushbu algoritmga qaratilgan ko‘zga ko‘ringan tahlil amalga oshirilmagan va u shuning uchun xavfsiz deb qaraladi. Mualliflarning ta’kidlashicha kalit ketma-ketligining davri 2^{256} dan katta.

SOSEMANUK sinxronlashgan oqimli shifrlash algoritmi bo‘lib, kalit uzunligi mos ravishda 128 yoki 256 bitli va 128 bitli IV dan foydalanadi. Biroq, barcha kalit uzunliklari uchun bir xil 128 bit xavfsizlik darajasini taqdim qiladi. Ushbu algoritm o‘zida SNOW 2.0 oqimli shifri va Serpent blokli shifrlarni ayrim elementlarini mujassam qilgan. Ushbu algoritm SNOW 2.0 algoritmiga qaraganda tezkor hisoblanadi. Ushbu algoritm LFSR va FSR foydalanib, 32 bitli so‘zlar ustida amallar bajaradi. Ushbu algoritmning kalitlarni o‘rnatish bosqichi uchun 24 raundli Serpent algoritmi ishlatilgan. Ushbu algoritmni dasturiy tomondan amalga oshirish o‘rtacha 2000-5000 baytni talab qilsa, qurilmada amalga oshirish uchun 18819 Geni talab qiladi.

Qurilmaga mo‘ljallangan oqimli shifrlash algoritmlari – ikkinchi guruh algoritmlari. Grain oqimli shifrlash algoritmi qurilmaga amalga oshirish uchun mo‘ljallangan bo‘lib, sinxronlashgan turdagi algoritm hisoblanadi. Ushbu algoritm LFSR va nozichiqli filterlash funksiyasidan iborat. LFSR minimal kalit ketma-ketlik davrini va chiqishdagi muvozanatni kafolatlaydi. Filterlash funksiyasi NFSR turida bo‘lib, shifrning nozichiqligini kafolatlaydi. LFSR dan chiqqan bitlar NFSRning kirish bitlari bilan qo‘shilib, holatning muvozanatlaydi.

Grain oqimli shifrlash algoritmi qurilmaga mos bo‘lishi uchun bitga qaratilgan bo‘lib, oddiy amalga oshirish 1 bit/siklni taqdim etadi. Biroq, ushbu algoritmda tezkorlikni oshirish uchun so‘zlar ustida amallarni bajarish imkoniyati mavjud. Biroq, bu imkoniyatga erishish uchun qurilma imkoniyatini yaxshilash talab etiladi. Bu holda tezkorlikni 16 bit/ siklgacha yetkazish mumkin. Ushbu algoritm A5/1 va

E0 algoritmlari kabi xavfsizlik darajasini ta’minlasada, buning uchun kichik qurilma imkoniyatini talab qiladi.

Grain algoritmi 80 bitli kalitlar va 64 bitli IV dan foydalanadi. Ushbu algoritmni 1 bit/siklda amalga oshirish uchun 1294 GE va 16 bit/siklda amalga oshirish uchun esa 3239 GE talab qilinadi. Dasturiy ko‘rinishda amalga oshirishda, 1 bit/sikl holatni ifodalash 778 bayt kod hajmiga teng bo‘lib, shifrni sozlash uchun 107366 sikl va natijani chop etish uchun 617 sikl talab qiladi.

Trivium shifrlash algoritmi ham ikkinchi guruhga tegishli algoritm bo‘lib, eSTREAM konkursining finalisti hisoblanadi va u LWC (ISO/IEC 29192-3:2012) uchun standartlashtirilgan. Ushbu algoritmni loyihalovchilari oqimli shifrlarni qanday qilib uning xavfsizligi, tezkorligi va moslashuvchanligini yo‘qotmasdan soddalashtirish mumkin degan savolga javob topishga harakat qilgan. Ushbu algoritm sinxronlashgan turga tegishli bo‘lib, 80 bitli kalitlar va 80 bitli IV dan foydalanadi. Ushbu algoritmda uchta SHR mavjud bo‘lib, ular algoritmda nozichiqlikni ta’minlab bergan.

Qurilma ko‘rinishda ushbu algoritmni amalga oshirish uchun standart CMOS (Complementary metal-oxide semiconductor) texnologiyasida 2017 GE talab qilingan bo‘lsa, talabga ko‘ra C2MOS texnologiyasida amalga oshirish uchun 749 GE talab qilingan.

O‘zi – sinxronlashuvchi oqimli shifrlar sanoat uchun sinxronlashgan algoritmlar kabi zarur hisoblanmasligini yuqoridagi tahlil natijalari ko‘rsatib o‘tildi. Xavfsiz sinxronlashgan shifrlar o‘rnatilgan shifrlar uchun asosiy tanlov hisoblanadi. Oqimli shifrlarda esa nochiziqli funksiya muhim hisoblanib, algoritm bardoshligini ta’minlashda muhim omildir.Autentifikatsiyalash imkoniyatiga ega shifrlar ham muhim bo‘lgan autentifikatsiya teglarini taqdim qiladi. Biroq, ushbu shifrlash sxemalari qator hujumlarga bardoshsiz bo‘lib, ularni yaratishdagi asosiy to‘siqlardan biri hisoblanadi. Shuning uchun mazkur muammoni bartaraf etishda odatda “shifrlash-keyin-MAC” sxemasidan keng foydalaniladi va bu odatiy autentifikatsiyalash imkoniyatiga ega shifrlarga qaraganda bardoshli xavfsizlikni taqdim qiladi.

III. Natijalar. *Amalga oshirilish darajasini baholash.* Oqimli shifrlash algoritmlarini 1-jadvaldagi kabi tahlillash, ularga to‘liq bahoni bermaydi. Xususan, bu o‘rinda amalga oshirishdagi ma’lumotlarni keltirish mumkin. Shu sababli, yuqori tahlil qilingan algoritmlarning qurilmada va dasturiy ko‘rinishda amalga oshirishdan olingan natijalar bilan quyida tanishib chiqiladi.

1-jadval. Tahlil qilingan shifrlarning umumiy xususiyatlari

Shifr nomi	Kalit uzunligi (bit)	Blok uzunligi (bit)	IV	Turi	Tahlili/ hujumlar
RC4	8-2048	1	-	ARX	Kalitga bog‘liq hujum, WEP dagi hujum
A5/1	54, 64	-	0	LSFR	Ma’lum ochiq matnga asoslangan hujum, time-memory tradeoff hujumi
E0	128	-	0	SHR	Bluetooth protokoliga asoslangan hujum
AES	128, 192, 256	128	0	SPN	Biclique kriptotahlili
Rabbit	128	128	-	Xaotik jadvallar + sodda amallar	Amaliy buzish hujumlari
Grain	80, 128	1, 16	64, 96	LFSR + NFSR	Differensial buzish hujumlari
Trivium	80	1, 8, 16	80	3 SHR	Takomillashgan differensial buzish hujumlari
Salsa	128, 256	32, 512	64, 128	ARX	Soddalashtirilgan versiyalariga hujumlar
HC	128, 256	-	128, 256	2 ta katta jadval	Turli kriptotahlil usullari
SOSEMANUK	128, 256	640, 32	64	LFSR+FSM	Takomillashgan differensial buzish hujumlari
MICKEY 2.0	80, 128	1	0-80, 0-128	Galua LFSR + NFSR	Takomillashgan differensial buzish hujumlari, kalitga bog‘liq hujumlar
Enocoro	80, 128	1	64	PRNG	Turli kriptotahlil usullari
Rabbit-MAC	128	128	-	Xaotik jadvallar + sodda amallar	Rabbit algoritmidagi hujumlar
BEAN	80	2	64	FCSR+S jadval	Holatni tiklash hujumlari
Hummingbird	256	16	64	Gibrid	Ko‘plab hujumlar
WG-7	80	1	81	LFSR+WG	Differensial hujumlar
TinyStream	128	-	-	TPM	-
Hummingbird-2	128	16	64	Gibrid	Kalitga bog‘liq hujumlar
Grain-128a	128	1	96	LFSR+NFSR	Differensial buzish hujumlari
A2U2	56	1	-	LFSR+2 NFSR	Ultra samarali tanlangan ochiq matnga asoslangan hujum
Quavium	80	1	80	4 Trivium algoritmidagi kabi SHR	-
Cavium	80	1	80	CA	-
ASC-1	128	128	56	SPN (CFB ga o‘xshash rejim)	Chegaralangan xavfsizlik
WG-8	80	1, 11	80	LFSR+WG	Kalitni tiklash hujumlari
CAR30	128	128	120	CA	-
ALE	128	128	128	SPN	Kriptohujumlar bilan obro‘sizlantirilgan
ACORN	128	-	128	6 LFSR	Moslashgan tanlangan ochiqmatnga asoslangan hujum
Sablier	80	-	80	ARX	Amaliy holatni tiklash hujumi

Qurilma ko‘rinishda amalga oshirish natijalari. Oqimli shifrlarni amalga oshirish kerak bo‘lgan qurilma muhiti cheklangan bo‘lib, [11] manbada mualliflar tomonidan Verilog tilida 5 ta oqimli shifrlash algoritmlari amalga oshirilgan. Bunda foydalanilgan qurilma arzon bo‘lgan Xilinx Spartan3 XC3S1000 FPGA (7680 qatlam (slices), 630 MHz, 55 KB RAM) qurilmasidan foydalanilgan.

Ushbu qurilmada amalga oshirilgan algoritmlarni baholashda o‘tkazish qobiliyati (throughput, MBps), kutish qiymati (latency, sikl/blok), maksimal chastota (maximum frequency, MHz), quvvat (power, W) va talab qilingan triggerlar hamda qatlam (flip-flops va slices) o‘lchovlari asosida baholangan. Quyida keltirilgan 1.2 – jadvalda tanlab olingan algoritmlarning yuqorida keltirilgan FPGA muhitida amalga oshirish natijalari keltirilgan. Algoritmlar sifatida AES, Enocoro-128, WG-8, Salsa20 va HC-256 lar tanlangan.

1.2 – jadval. FPGA muhitida algoritmlarning omillar bo‘yicha tahlili (qaysi holda yaxshi ko‘rsatkich bo‘lishi ham keltirilgan)

Shifr	Kalit uzunligi (bit)	Blok uzunligi (bit)	IV (bit)	Kutish qiymati (sikl/blok)	O‘tkazish qobiliyati (MBps)	Mak. Chastota (MHz)	Quvvat (W)	FF	Qatlamlari	O‘tkazish qobiliyati/ qatlamlari
Yaxshisi	-	-	-	Pasti	Yuqorisi	-	Pasti	Pasti	Pasti	Yuqori
WG-8	80	1	80	1	2112	192	0.016	207	398	0.66
Enocoro-80	80	1	64	1	900	118	0.008	239	292	0.38
Enocoro-128	128	1	64	1	1200	149	0.008	362	442	0.33
AES	128	128	-	226	8754	77	0.078	781	5948	0.18
WG-8	80	11	80	1	190	190	0.005	85	137	0.17
Salsa20	256	32	64	2	990	19.4	0.012	1286	2036	0.06
HC-128	128	512	128	-	-	-	-	-	>>262000	-

Bundan tashqari, ushbu algoritmlarni ASIC (Application specific integrated circuit) muhitida amalga oshirish natijalari ham keltirilgan. Mazkur holda tahlillash omili sifatida o‘tkazish qobiliyati, GE va yuqori sifatlilik (figure of merit, FOM)lar tanlab olingan. Bunda FOM kattaligi o‘$tkazish\ qobiliyati/_{GE^2}$ tarzida hisoblangan va algoritmning qurilmada amalga oshirishdagi sifat darajasini ko‘rsatgan. Mazkur muhitda olingan tahlil natijalari esa 1.3 – jadvalda keltirilgan.

1.3 – jadval. ASIC muhitida algoritmlarning omillar bo‘yicha tahlili (qaysi holda yaxshi ko‘rsatkich bo‘lishi ham keltirilgan)

Shifr	Kalit uzunligi (bit)	Blok uzunligi (bit)	IV (bit)	Kutish qiymati (sikl/blok)	Har 100 KHz da o‘tkazish qobiliyati (MBps)	Tex. (µm)	Maydoni (GE)	FOM
Yaxshisi	-	-	-	Pasti	Yuqorisi	-	Pasti	Yuqorisi
WG-8	80	1	80	1	100	0.65	1786	0.00391
Enocoro-80	80	1	64	1	-	0.09	2700	-
Enocoro-128	128	1	64	1	800	0.09	4100	0.00594
AES	128	128	-	226	56.64	0.35	2400	0.00122
WG-8	80	11	80	1	1100	0.65	3942	0.00884
Salsa20	256	32	64	2	99	0.13	12126	0.00008
HC-256	128	512	128	-	-	0.13	>>524000	-

WG-8, Enocoro va AES algoritmlar o‘rnatilgan tizimlar uchun mos bo‘lgan qulay amalga oshirilish imkoniyatiga ega hisoblanadi (3000 dan kam bo‘lgan GE). Bular orasida WG-80 eng ixcham va samarali algoritm hisoblangan. Enocoro algoritmi ham yaxshi amalga oshirilish darajasiga ega va LWC muhitida amalga oshirish mumkin bo‘lgan standartlashtirilgan algoritmdir. AES algoritmi yuqori xavfsizlik darajasini qayd qilsa ham, yuqori energiya sarfiga ham ega. Qolgan Salsa20 va HC algoritmlari esa o‘rnatilgan qurilmalar uchun mos emas.

Dasturiy vosita ko‘rinishda amalga oshirish natijalari. Qurilmada amalga oshirishga o‘xshash holda, mualliflari tomonidan ayrim oqimli shifrlash algoritmlari C dasturlash tilida kredit karta o‘lchamidagi o‘rnatilgan qurilma, BeagleBone (AM3359 ARM Cortex A8 single core CPU, 720 MHz, 256 MB RAM, Ubuntu OS) muhitida amalga oshirildi. Barcha amalga oshirilishlar umumiy bo‘lgan testlash omillari asosida baholandi. Mazkur holda baholash omillari sifatida ROM, RAM va mujassamlashgan o‘lchov (combine metric, CM) kattaliklaridan foydalanilgan. ROM va RAM kattaliklari kod va vaqt-xotira kattaliklarini Kbaytda o‘lchaydi. CM kattaligi esa $(ROM \times shifrlashdagi\ sikl)/blok$ o‘lchamini ko‘rsatadi. Dasturiy vosita ko‘rinishda amalga oshirish uchun AES/ AES-CTR, Enocoro-128, WG-8, Salsa20 va HC-128 algoritmlari tanlab olingan. 1.4-jadvalda dasturiy vositalarni amalga oshirishdan olingan natijalar keltirilgan.

IV.XULOSA. Dasturiy vosita ko‘rinishda amalga oshirishda Salsa20 algoritmi tezkorlik va ishga tushirishning qisqaligi bilan qolganlaridan ajralib turgan. Enocoro va WG-8 algoritmlari ham kam kod hajmi va xotira talab qilishi bilan ajralib turgan. Eng tezkor shifrlash algoritmi HC bo‘lgan bo‘lsa, eng sekin algoritm AES standarti bo‘lgan.

1.4 – jadval

Dasturlash muhitida algoritmlarning omillar bo‘yicha tahlili (qaysi holda yaxshi ko‘rsatkich bo‘lishi ham keltirilgan)

Shifr	Kalit uzunligi (bit)	Blok uzunligi (bit)	IV (bit)	Ishga tushirish (sikl)	Shifrlash (sikl)	ROM (Kbayt)	RAM (Kbayt)	Har 720 MHz da o‘tkazish qobiliyati (MBps)	CM
Yaxshisi				Pasti	Pasti	Pasti	Pasti	Yuqori	Pasti
Salsa20	128	512	64	460	29491	4.8	8.27	12.5	276
Salsa20	256	512	64	460	29729	4.8	8.35	12.4	278
Enocoro-128	128	1	64	4870	138	3.8	7.56	5.2	526
WG-8	80	1	8	1379	69	6.6	0.59	10.4	456
HC-128	128	512	128	2082876	17388	77.2	16.58	21.2	2621
AES	128	128	-	6953	20480	22.2	88	4.5	3552
AES-CTR	128	128	128	469.6	21942	22.3	88.5	4.2	3822

Xulosa o‘rnida shuni aytish mumkinki, xavfsiz bo‘lgan algoritmni tanlash degani butun ilovani xavfsiz bo‘ldi degani emas. Boshqa so‘z bilan aytganda, butun ilovani loyihalash davomida nafaqat algoritmlarning xavfsizligiga, balki, ularning mosligiga va to‘g‘ri birlashtirilganiga ham e’tibor berish kerak hisoblanadi.

Foydalanilgan adabiyotlar ro‘yxati

1. Klein A. Introduction to stream ciphers, Stream Ciphers. Springer, 2013; pp. 1–13.
2. Bellovin S.M, Miller F. Inventor of the one-time pad. Cryptologia 2011; 35(3): 203–222.
3. Shannon CE. Communication theory of secrecy systems. Bell System Technical Journal 1949; 28(4): 656–715.
4. Daemen J, Lano J, Preneel B. Chosen ciphertext attack on SSS. eStream Report, Article 2005/044, 2005.
5. Raxmatullayebich R. I. STREAM ENCRYPTION ALGORITHMS AND THE BASIS OF THEIR CREATION //CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES. – 2022. – T. 3. – №. 12. – C. 165-173.
6. Rakhmatullaev I. Evaluation of new NSA stream encryption algorithm by integrated cryptanalysis method //Scientific Collection «InterConf». – 2023. – №. 164. – C. 242-248.
7. Rahmatullayev I. the A NEW KEY STREAM ENCRYPTION ALGORITHM AND ITS CRYPTANALYSIS: The new stream encryption algorithm (NSA-New Stream Algorithm) is proposed in this work. The input parameters are considered a 128-bit secret key and 128-bit initialization vectors in the new algorithm. A 64-bit line is generated in each round as the output value. The architecture of the algorithm is particularly suitable for efficient hardware implementations, together with this, this algorithm is also suitable for software implementation ... //Scientific and Technical Journal of Namangan Institute of Engineering and Technology. – 2023. – T. 8. – №. 1. – C. 146-157.
8. Rakhmatullaevich R. I., Mardanokulovich I. B. Analysis of cryptanalysis methods applied to stream encryption algorithms //Artificial Intelligence, Blockchain, Computing and Security Volume 1. – CRC Press, 2024. – C. 393-401.
9. Rakhmatullaev I. Self-synchronizing (asynchronous) Stream Encryption Algorithms //Scientific Collection «InterConf». – 2023. – №. 164. – C. 249-254.
10. Khudoykulov Z. T., Rakhmatullaev I. R., Umurzakov O. S. H. NSA algoritmining akslantirishlari tanlanishining xavfsizlik talablarini bajarilishidagi o ‘rni //INTERNATIONAL JOURNAL OF THEORETICAL AND APPLIED ISSUES OF DIGITAL TECHNOLOGIES. – 2023. – T. 6. – №. 4. – C. 97-101.
11. Xudoyqulov Z. T., Rahmatullayev I. R., Boyqo‘ziyev I. M. Bardoshli statik S-bokslarni generatsiyalash algoritmi //INTERNATIONAL JOURNAL OF THEORETICAL AND APPLIED ISSUES OF DIGITAL TECHNOLOGIES. – 2023. – T. 5. – №. 3. – C. 57-66.
12. Rahmatullayev I. R. Algebraik kriptotahlil usuli va uning oqimli shifrlash algoritmlariga qo‘llanish asoslari: Algebraic Cryptanalysis Method and Basics of its Application to Stream Encryption Algorithm //International Journal of Theoretical and Applied Issues of Digital Technologies. – 2023. – T. 4. – №. 2. – C. 96-102.
13. Rahmatullayev I. R. Oqimli shifrlash algoritmlari va ularni vujudga kelish sabablari //International Journal of Theoretical and Applied Issues of Digital Technologies. – 2022. – T. 2. – №. 2. – C. 119-128.
14. Raxmatullayevich R. I. OQIMLI SHIFRLASH ALGORITMLARI TAHLILI //Новости образования: исследование в XXI веке. – 2023. – T. 1. – №. 6. – C. 889-893.