9. Tolipov, N., Xudoynazarov, Q., & Munavarjonov, S. (2023). ОБ ОДНОЙ НЕКОРРЕКТНОЙ ЗАДАЧЕ ДЛЯ БИГАРМОНИЧЕСКОГО УРАВНЕНИЯ В ПОЛУШАРЕ. *Research and implementation*.
10. To‘xtasinov, D. F., & qizi Abdullayeva, S. H. (2023). MATEMATIKA DARSLARIDA IJODIY TAFAKKURNI RIVOJLANTIRISH SHARTLARINING DIDAKTIK KOMPLEKSINI AMALIYOTDA QO‘LLASH YO‘LLARI. *Educational Research in Universal Sciences*, *2*(2), 613-616.

SM4 SHIFRLASH ALGORITMINI APPARAT AMALGA OSHIRISH USULLARI

Olimov Iskandar Salimboyevich,
Korabayev Eldor Alijonovich,
Karimov Abduqodir Abdusalomovich
Toshkent axborot texnologiyalari universiteti
karimovabduqodir041@gmail.com

Annotatsiya: Ushbu maqolada SM4 shifrlash algoritmini amalga oshirish usullariga bag‘ishlangan bo‘lib, unda SM4 shifrlash algoritmini ma’lumotlarni maxfiyligini ta’minlashdagi o‘rni, ishlash funksiyasi shu bilan birga aparat amalga oshirish usullari va ularni tahlili keltirilgan.

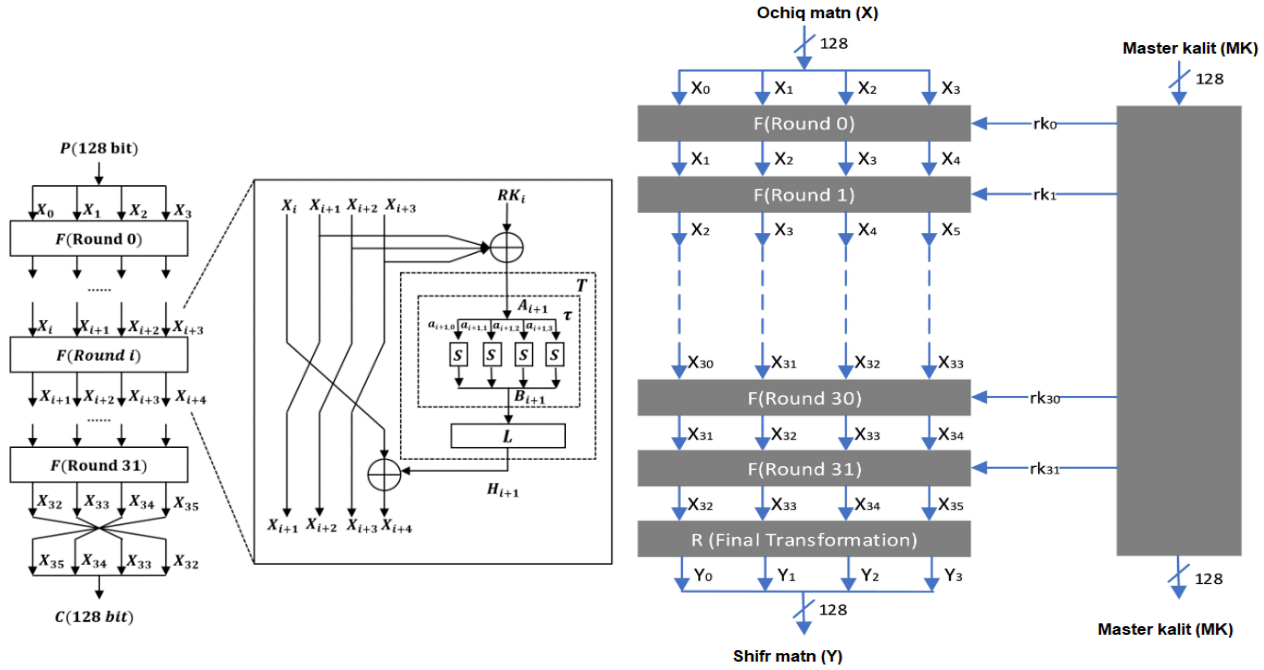
Kalit so‘zlar: SM4, feystel tarmog‘i, FPGA, Elektron Codebook (ECB), Cipher Block Chaining (CBC).

SMS4 nomi bilan ham tanilgan SM4 shifr 2007 yilda Xitoy Milliy Kriptografiya Byurosi tadqiqotchilari tomonidan ishlab chiqilgan. U Xitoy uchun ma’lumotlar maxfiyligini ta’minlashda foydanilgan shifrlash standarti DES va uning vorisi o‘rnini bosuvchi milliy standart shifrlash algoritmi sifatida ishlab chiqilgan.

SM4 shifrlash algoritmi feystel tarmog‘iga asoslangan bo‘lib, uni blok uzunligi 128 bitni tashkil etadi, bu 16 baytga teng. Bu shuni anglatadiki, SM4 shifrlash va shifrni ochish jarayonida bir vaqtning o'zida 128 bitli bloklarda foydaniladi [1,2].
Umumiy olganda 128 bitli blok o'lchami zamonaviy blok shifrlari uchun keng tarqalgan tanlovdir, chunki u xavfsizlik va samaradorlik o'rtasidagi muvozanatni ta'minlaydi. Blokning kattaroq o'lchami ko'proq mumkin bo'lgan kirishlar to'plamini joylashtirish orqali xavfsizlikni oshirishi mumkin, ammo u hisoblashning murakkabligini oshirishi va qayta ishlashni sekinlashtirishi mumkin.1-rasm. Feystel tarmog‘iga asoslangan SM4 shifrlash algoritmi.

Aksincha, kichikroq blok o'lchami samaraliroq bo'lishi mumkin, ammo kirish maydoni cheklanganligi sababli ma'lum turdagi hujumlarga moyil bo'lishi mumkin.

SMS4 algoritmi sifatida ham tanilgan SM4 shifrlash algoritmi ma'lumotlarni shifrlash va shifrini ochish uchun ishlatiladigan simmetrik blokli shifrdir. Bu Xitoyda keng tarqalgan bo'lib qabul qilingan standart bo'lib, turli ilovalarda, jumladan xavfsiz aloqa va ma'lumotlarni himoya qilishda qo'llaniladi. Bu maqolada SM4 algoritmining apparat amalga oshirish jihatlari haqida umumiy ma'lumot keltirilgan [2,3]:



2-rasm. SM4 shifrlash jarayoni

SM4 shifrlash algoritmini aparat amalga oshirish:

FPGA: FPGA apparatda SM4 ni amalga oshirish uchun ishlatilishi mumkin. FPGA-ga asoslangan ilovalar yuqori unumdorlikni taklif qiladi va moslashuvchanlik uchun qayta dasturlanishi mumkin.

ASIC: Ilovaga oid integral sxemalar (ASIC) ishlash va quvvat samaradorligi uchun optimallashtirilgan maxsus apparat dasturlarini taqdim etadi. ASIC ko'pincha SM4 algoritmi xavfsiz chiplar yoki kriptografik modullar kabi maxsus apparat qurilmalariga o'rnatilishi talab qilinadi.

Shuni ta'kidlash kerakki, SM4 kabi kriptografik algoritmlarni qo'llashda xavfsiz kodlash, kalitlarni boshqarish va algoritm konfiguratsiyasi uchun o'rnatilgan eng yaxshi amaliyotlarga amal qilish juda muhimdir. Bundan tashqari, amalga oshirishda aniqlanishi mumkin bo'lgan har qanday zaiflik yoki zaifliklarni bartaraf etish uchun muntazam xavfsizlik talablarini oshirish kerak [2,3].

SM4 simmetrik blokli shifrlash algoritmi bo'lib, Xitoy standart shifrlash algoritmi bo‘lib, tuzilishi va ishlashi jihatidan AES (Advanced Encryption Standard) algoritmiga o‘xshaydi. SM4 shifrlash yoki har qanday blokli shifrlash algoritmini tahlil qilishda odatda bir nechta jihatlar hisobga olinadi:

Xavfsizlik: Kriptografik algoritmlar turli xil hujumlarga chidamliligiga qarab baholanadi. SM4 xavfsizligi kriptografik hamjamiyat tomonidan keng tahlil qilingan. U ma'lum hujumlarga, shu jumladan differentsial va chiziqli kriptoanalizga qarshi chidamliligini ta'minlash uchun jiddiy tekshiruv va baholashdan o'tdi.

Ishlash tartibi: SM4 ham boshqa blokli shifrlash algoritmlari kabi Elektron Codebook (ECB), Cipher Block Chaining (CBC), Counter (CTR) yoki Galois/Counter Mode (GCM) rejimlar bilan birgalikda ishlatiladi.

Amalga oshirish: Algoritmning amalda bajarilishi juda muhim. Algoritmning to'g'ri va xavfsiz ishlashini ta'minlash uchun u eng yaxshi amaliyotlar va xavfsizlik ko'rsatmalariga amal qilishi kerak [1,3].

Kriptanaliz: Kriptanaliz - bu zaif yoki zaif tomonlarni topish maqsadida kriptografik algoritmlarni o'rganishdir. *Kriptonalistlar* SM4 kabi algoritmlarni tahlil qilib, potentsial hujumlar yoki ularning xavfsizligiga putur etkazadigan kamchiliklarni aniqlaydilar.

SM4 shifrlash yoki har qanday blokli shifrlash algoritmini tahlil qilishda ushbu omillarni hisobga olish va tegishli tadqiqot hujjatlari, kriptografik standartlar va professional kriptograflarning tajribasi bilan maslahatlashish zarur.

SM4 shifrlash uchun keng tarqalgan FPGA qurilmalari uchun taqqoslash jadvali:

1-jadval

SM4 shifrlash uchun keng tarqalgan FPGA qurilmalari tahlili

FPGA qurilmasi	*Ishlab chiqaruvchi*	*Asosiy xususiyatlar*	*Mavjud ligi*
Xilinx Ultra Scale+	Xilinx	Integratsiyalashgan kriptografik funksiyalarga ega yuqori samarali FPGA. Uskuna IP orqali SM4 shifrlash tezlashuvini qo'llab-quvvatlaydi. Yuqori tezlikdagi ma'lumotlarni qayta ishlash va moslashuvchan dasturlash imkoniyatini taklif etadi.	Keng tarqal gan
Intel Stratix 10	Intel	O'rnatilgan xavfsizlik xususiyatlariga ega yuqori sig'imli FPGA. Maxsus shifrlash IP yordamida SM4 shifrlash tezlashuvini qo'llab-quvvatlaydi. Yuqori ishlash va quvvat samaradorligini taklif qiladi.	Keng tarqal gan
Panjara ECP5	Panjara yarimo'tkaz gich	Konfiguratsiya qilinadigan mantiqiy resurslarga ega kam quvvatli FPGA. Maxsus RTL dizaynlari orqali SM4 shifrlashni qo'llab-quvvatlaydi. Kam quvvat sarflaydigan va arzon narxlardagi ilovalar uchun javob beradi.	Keng tarqal gan
Microsemi SmartFusio n2	Mikrochip	O'rnatilgan ARM Cortex-M3 protsessori va xavfsizlik xususiyatlariga ega FPGA. Maxsus RTL dizaynlari va dasturiy ta'minotni amalga oshirish orqali SM4 shifrlashni qo'llab-quvvatlaydi. FPGA moslashuvchanligi va mikrokontroller imkoniyatlarining kombinatsiyasini taklif qiladi.	Keng tarqal gan
QuickLogic EOS S3	QuickLogic	Integratsiyalashgan ARM Cortex-M4 protsessorli ultra kam quvvatli FPGA. Maxsus RTL dizaynlari va dasturiy ta'minotni amalga oshirish orqali SM4 shifrlashni qo'llab-	Keng tarqal gan

		quvvatlaydi. Quvvatga sezgir ilovalar uchun mo'ljallangan.	

Ushbu FPGA qurilmalari turli imkoniyatlar, ishlash darajalari va quvvat talablarini ta'minlaydi. Muayyan ehtiyojlaringizga qarab, siz loyiha talablari va byudjetingizga eng mos keladigan FPGA qurilmasini tanlashingiz mumkin. Batafsil texnik ma'lumotlar va ushbu qurilmalar yordamida SM4 shifrlashni FPGA dizaynlariga integratsiya qilish bo'yicha ko'rsatmalar uchun tegishli ishlab chiqaruvchining hujjatlari va qo'llab-quvvatlash manbalarini ko'rib chiqish tavsiya etiladi.

Axborot texnologiyalarini rivojlanib borishi o‘znavbatida axborotni maxfiyligini ta’minlashga qaratilgan e’tibor ortishiga sabab bo‘lmoqda. Ushbu maqolada SM4 shifrlash algoritmini ishlash imkoniyatlari, apparat amalga oshirish usullari va ularni tahlili ishlab chiqilgan. Ma’lumotlarni maxfiyligini ta’minlashda SM4 shifrlash algoritmini dasturiy va apparat ko‘rinishida amalga oshirish orqali yuqori samaradorlikka erishish mumkin.

Foydalanilgan adabiyotlar ro‘yxati:

1. I.S.Olimov. (2023). SM4 SHIFRLASH ALGORITMINI DASTURIY AMALGA OSHIRISH USULLARI. *GOLDEN BRAIN*, *1*(18), 166–171

2. Boriyev Y.A., Sadikov M.A., Khamidov SH.J., “Internet of things architecture and security challenges ICISCT 2020 confrence international conferencye on information sciyencye and communications technologiyes 4,5,6 November.

3. Abed, Sa'ed, et al. "Performance evaluation of the SM4 cipher based on field-programmable gate array implementation." *IET Circuits, Devices & Systems* 15.2 (2021): 121-135.

TANIB OLISH MODULLARINI DASTURIY AMALGA OSHIRISH

Mamaraimov Abror Kamoliddin o‘g‘li,
Choryorqulov G‘iyos Husan o‘g‘li,
Normatov Nizomiddin Kamoliddin o‘g‘li
O‘zbekiston Milliy Universiteti Jizzax filiali
normatov@jbnuu.uz

Annotatsiya: Tanib olish modullarini dasturiy jihatdan amalga oshirish hamda nutqni tanib olish moduli ishini sifatini baholash ishlarini olib borish. Nutq signaliga dastlabki ishlov berish va ularni neyron tarmoqlarida o‘qitishga tayyorlash jarayonini avtomatlashtiruvchi dasturiy modul ishlab chiqildi. Ushbu dasturiy modul yordamida katta xajmdagi nutq ma’lumotlarini tarmoqga kirish standartiga moslash imkoniyatini beradi.

Kalit so‘zlar: Wav, CTC, *MFCC,* WER, CER , Epoch