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

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

PRESENT YENGIL VAZNLI KRIPTOGRAFIK ALGORITMINING TAHLILI

Xudoykulov Zarif Turakulovich,
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, “Kriptologiya” kafedrasi mudiri, Phd.,dotsent, Toshkent, O‘zbekiston
e-mail: zarif.khudoykulov@tuit.uz

Qozoqova To‘xtajon Qaxramon qizi,
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti, “Kriptologiya” kafedrasi assistenti, Toshkent, O‘zbekiston
e.mail: qozoqovat1516@gmail.com

Annotatsiya. Ushbu maqolada IoT qurilmalari va ularda foydalaniladigan kam resurs sarfiga ega, yengil vaznli kriptografik algoritmlar haqida qiyosiy tahlil ma’lumotlari, bajarilgan tadqiqotlar natijalari keltirilgan. Xususan, PRESENT yengil vaznli shifrlash algoritmini ishlash bosqichlari, ushbu algoritmni SPEAK shifrlash algoritmi bilan bir xil muhitida (ya’ni, CrypTool 2.1dasturida) qiyosiy tahlil qilindi. Tahlil natijalari PRESENT yengil vaznli shifrlash algoritmini IoT qurilmalarida xavfsizlik masalalariga javob bera olishi uchun takomillashtirish va roundlar sonini kamaytirish kerakligini ko‘rsatdi.

Kalit so‘zlar: PRESENT, IoT, yengil vaznli kriptografiya, NIST, Simon, SPEAK, Katan, Klein

Kirish. Hozirgi kunda jadal rivojlanayotgan IoT (Internet of Things) texnologiyalari kundalik faoliyatda muhim o‘rin egallaydi. IoT bir-biri bilan bog‘langan bir nechta qurilmadan iborat bo‘lib, ular o‘zaro doimiy ravishda ma’lumot va axborot almashadilar. IoT texnologiyalari kengaygan sari, ularga qaratilgan xavfsizlik talablari ham kuchaymoqda. ThreatLabzning hisobotiga ko‘ra IoT qurilmalariga hujumlar yiliga 45 % oshmoqda [1]. Ushbu ma’lumotlar asosida, xavfsizlik talablarini kuchaytish maqsadida IoT texnologiyalari xavfsizligini asosi bo‘lgan yengil vaznli kriptografik (lightweight cryptography) algoritmlar samaradorligini oshirish va ularni takomillashtish masalasini dolzarb deb aytish mumkin.

Yengil vaznli kriptografiya bu hisoblash quvvati, xotira hajmi va energiya sarfi cheklangan qurilmalar uchun mo‘ljallangan kriptografik algoritmlar. Bu algoritmlarni yaratilish tarixi IoT texnologiyalari rivojlanish boshqichiga to‘g‘ri keladi. 2011-yilda NIST (National Institute of Standards and Technology) tomonidan tanlov o‘tkazildi. Ushbu tanlov davomida PRESENT, SIMON, SPECK, KATAN, va KLEIN kabi algoritmlar qatnashdi. Bu algoritmlar o‘zlarining kichik o‘lchamlari va kam resurslar talab qilishi bilan ajralib turardi va ularni bu xususiyatlari boshqa algoritmlardan ustunlik qildi.

Adabiyotlar tahlili va metodologiya. Mavzu doirasida ko‘plab adabiyotlar va maqolalar tahlil qilindi. Yengil vaznli shifrlash algoritmlarining tahlili va ularning samaradorligini oshirish borasida bir qancha tadqiqotlar o‘tkazilgan, PRESENT shifrlash algoritmi ham shular qatoridadir. Xususan, Muhammad Rana va boshqalar tomonidan [2] yozilgan maqolada IoT qurilmalarida resurs cheklanganlik sababi ularda qo‘llanilgan yengil vaznli shifrlash algoritmlarini tahlili keltirilgan. Bunda shu algoritmlarni xavfsizlik samaradorligi, tezlik va qurilmalardagi energiya sarfi bo‘yicha tahlillar amalga oshirilgan. Christophe De Canniere va boshqalar [3] tomonidan 32, 48 va 64 bitlik blok o‘lchamlarini qo‘llaydigan, 80 bitlik kalitdan foydalanadigan KATAN shifri ishlab chiqilgan. Ushbu algoritmda kalit qurilmaga o‘rnatib yuboriladi (burnt-in). Matn nusxasi registrga yuklanadi va shifrlash jarayoni boshlanadi.

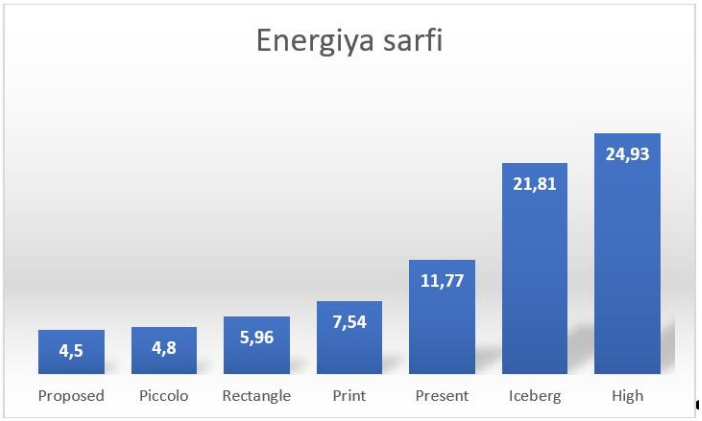
Julia Borghoff va boshqalar [4] tomonidan ishlab chiqilgan PRINCE shifri 64 bitlik blok o‘lchami va 128 bitlik kalitdan foydalanadi. Ushbu shifr kalitni matn bo‘ylab tarqatadi va kriptologik hujumlarning oldini olish uchun maxsus mexanizmlarga ega. Deukjo Hong va boshqalar [5] esa Feistel tarmog‘iga asoslangan shifrni ishlab chiqishgan. U ham 64 bitlik blok o‘lchami va 128 bitlik kalitdan foydalanadi. Algoritm oddiy XOR va siljitish (shift) operatsiyalarini F_0 va F_{31} funksiyalarida qo‘llaydi.

Ray Beaulieu va boshqalar [6] tomonidan har xil blok va kalit o‘lchamlariga ega bo‘lgan shifrlar ishlab chiqilgan. Ushbu shifrlar apparat va dasturiy tizimlarning protsessorlardagi tuzilishini takomillashtirishga mo‘ljallangan. Shifr modulyar qo‘shish, XOR, chapga va o‘ngga aylanish (circular shift) operatsiyalaridan foydalanadi. Yengil vaznli kriptografiya algoritmlari bo‘yicha sharh Kong Jia Hao va boshqalar tomonidan muhokama qilingan. Ular energiya va resurslarni samarali ishlatish uchun optimallashtirilgan algoritmlar haqida ma’lumot beradi.

Gauravm Bansod [7] tomonidan PRESENT-GRP gibrid usuli tushuntirilgan. Bu usulda kirish ma’lumotlari bloklari PRESENT S-box orqali tarqatilib, chiqish ma’lumotlari PRESENT-GRP algoritmi yordamida akslantirilib, keyin o‘rin almashtirish qatlamiga o‘tkaziladi. PRESENT-GRP algoritmi S-box 4x4 tuzilishda yaratilgan bo‘lib, murakkablik va energiya iste’molini kamaytirishga qaratilgan.

64-bitli qiymat ustida operatsiya bajarish uchun loyihalash shunday amalga oshirilganki, u faqat 16 ta 4-bitli PRESENT S-boxdan foydalanadi va PRESENT GRPga permutatsiya uchun uzatiladi. PRESENT-GRP gibrid strukturasining xotira talabi mavjud algoritmlarga nisbatan ancha kam. GRP P-box gatelar ekvivalentini kamaytirish uchun yetti bosqichdan foydalanadi. Bitlar quyidagicha guruhlanadi: birinchi guruh 0-bit va 64-bitni, ikkinchi guruh 1-bit va 65-bitni o‘z ichiga oladi va hokazo. Shifrlash algoritmlarining yengil vaznli apparat va dasturiy ta’minotda amalga oshirilishi haqida George Hatzivasilis va boshqalar [8] tomonidan ham muhokama qilingan.

Quvvat sarfi IoT qurilmalarida hozirda eng muhim omillardan biri. Ushbu talab doirasida Muhammad Rana o‘z maqolasida quyidagicha tadqiqot natijalarini e’lon qildi. 1-rasmda keltirilgan Proposed, Piccolo, Rectangle, Print, Present, Iceberg, High algoritmlarini quvvat sarfi ustunlar shaklida keltirilgan [2].



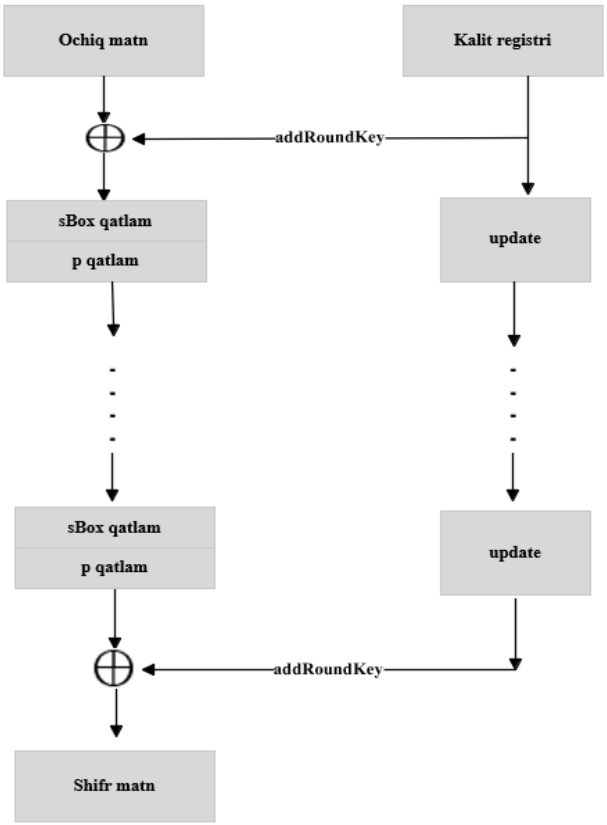
1-rasm. Turli yengil vaznli algoritmlarning energiya sarfi

Yengil vaznli algoritm tavsifi. PRESENT- bu yengil vaznli blokli shifrlash algoritmi bo‘lib, 2007-yilda Andrey Bogdanov va boshqalar tomonidan ishlab chiqilgan. Ushbu algoritm asosan apparat va dasturiy ta’minot resurslari cheklangan tizimlar, masalan, IoT qurilmalari, RFID texnologiyalari va sensor tarmoqlari uchun mo‘ljallangan. 2012-yilda Xalqaro Global Elektron Spetsializatsiya Komissiyasi (ISO/IEC) tomonidan nazorat qilingan va asosan yengil vaznli kriptografiya uchun moslashtirilgan.

Algoritmni afzalliklari. Kichik tranzistor soni, past energiya sarfi va xavfsizlikni ta’minlash uchun optimallashtirilgan. PRESENT algoritmi o‘zining ko‘plab afzalliklariga qaramay, bir nechta kamchiliklari mavjud. Dasturiy ta’minotda algoritmning shifrlash tezligi past. PRESENT asosan apparat muhitida samarali ishlash uchun mo‘ljallangan. Dasturiy ta’minotda ishlash tezligi boshqa yengil vaznli algoritmlarga nisbatan pastroq. Algoritmning keyingi kamchiligi bu uning kalit uzunligi. 80 bitlik kalit uzunligi uzoq muddatli xavfsizlik uchun yetarli emas, chunki hisoblash quvvatining oshishi bilan bruteforce texnologiyasi yordamida kalitni oshkor bo‘ladi. 128 bitlik PRESENT algoritmi mavjud lekin

80 bitli kalit uzunligi mavjud varianti ko‘proq ishlatiladi. Algoritm differensial va chiziqli kriptotahlillarga bardoshsiz. Algoritm 31 rounddan iborat bo‘lib, bu boshqa yengil vaznli shifrlash algoritmlariga nisbatan ko‘proq. Bu ko‘proq energiya sarfiga olib kelishi mumkin. Algoritm autentifikatsiya yoki ma’lumotlarning yaxlitligini ta’minlash uchun qo‘shimcha mexanizmlarni o‘z ichiga olmaydi. Bu uning ma’lum xavfsizlik talablari uchun mos emasligiga olib kelishi mumkin.

Ishlash prinsipi. PRESENT blokli shifrlash algoritmi SP (Substitution-Permutation Network) tarmog‘iga misol va u 31 raunddan iborat. Blok uzunligi 64 bitni tashkil qiladi va ikkita 80 va 128 bitli kalit uzunliga ega. Qo‘llanilish sohalarini hisobga olgan holda, 80-bitli kalit uzunligdagi versiyasi keng qo‘llaniladi. Bu odatda past darajadagi xavfsizlik (low-security) ilovalarida talab qilinadigan darajada xavfsizlikni ta’minlaydi.



2-rasm. Present shifrlash algoritmini tavsifi

Algoritm 31 round quyidagilarni o‘z ichiga oladi round kaliti $K_i$uchun $1 \le i \le 32$ ni kiritish uchun XOR amali, bunda K_{32} post-whitening uchun ishlatiladi, chiziqli bit darajasidagi permutatsiya va chiziqsiz almashtirish qatlami. Chiziqsiz qatlamda bitta 4-bitli S-box ishlatiladi u har bir roundda 16 marta parallel ravishda qo‘llaniladi. Shifrlash algoritmi 1-rasmda tasvirlangan va har bir bosqich ketma-ketligi quyidagicha aniqlangan.

$addRoundKey$. Berilgan round kalit $K_i = \kappa_{63}^i \dots \dots \kappa_0^i$ uchun $1 \le i \le 32$ va joriy holatda $b_{63} \dots \dots b_0$, addRoundKey $0 \le j \le 63$ iborat,

$$b_j \to b_j \oplus \kappa_j^i \qquad (1)$$

$sBox\ qatlam$. S-box PRESENT shifrlash algoritmida 4-bitli S: $F_2^4 \longrightarrow F_2^4$ bu S-boxning o‘n oltilik tizimida quyidagi 1-jadvalda berilgan.

1-jadval. S jadvalning o‘n oltilik tizimda qiymati

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S(x)	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

$sBoxLayer$ uchun joriy holat $b_{63} \dots \dots b_0$ o‘n oltita 4 bitli so‘zlar sifatida ko‘rib chiqiladi. $w_{15} \dots \dots w_0$, bu yerda $w_i = b_{4*i+3}||b_{4*i+2}||b_{4*i+1}||b_{4*i}$ uchun $0 \le i \le 15$ va chiquvchi $S(w_i)$ qiymatlarini taqdim etadi.

$pLayer$. PRESENT shiflash algoritmida 2-jadvalda permutatsiya jadvali berilgan. i bit $P(i)$ ni qiymatlarini qabul qiladi.

2-jadval. Permutatsiya jadvali

I	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
P(i)	0	16	32	48	1	17	33	49	2	18	34	50	3	19	35	51
I	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
P(i)	4	20	36	52	5	21	37	53	6	22	38	54	7	23	39	55
I	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
P(i)	8	24	40	56	9	25	41	57	10	26	42	58	11	27	43	59
I	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
P(i)	12	28	44	60	13	29	45	61	14	30	46	62	15	31	47	63

PRESENT algoritmi 80 yoki 128 bitli kalitlar mavjud, bu yerda 80-bitli kalit uchun ishlash ketma-ketligi keltirilgan. Foydalanuvchi tomonidan taqdim etilgan kalit K registrida saqlanadi va quyidagicha ifodalanadi:

$$K = k_{79}k_{78} \dots \dots k_0 \qquad (2)$$

Bu yerda, k_{79} - eng boshida (chapdagi) bit va k_0- eng oxirgi (o‘ngdagi) bitni bildiradi.

Raund kalitini olish (Round Key Extraction)

Har bir raundda 64-bitli raund kaliti $K_i$olinadi, bu esa K registrining hozirgi holatining chapdagi 64 bitidan iborat.

$$K_i = k_{79}k_{78} \dots \dots k_{16} = \kappa_{63} \dots \dots \kappa_0 \qquad (3)$$

Bu yerda, K_i 80 bitli kalitni generatsiya qiladi va uning 64 ta bitlari K registrining chap tomonidan olinadi.

Kalitni yangilash (Key Update):

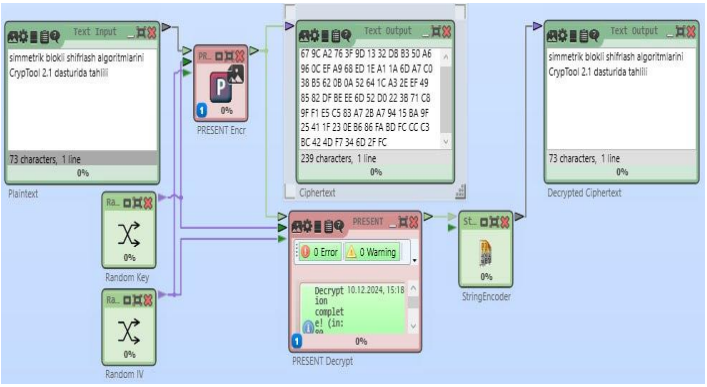
Raund kaliti K_i generatsiya qilingach K registri yangilanadi. Yangilash jarayoni quyidagicha amalga oshiriladi.

K registrining bitlari bir pozitsiyaga chapga aylantiriladi. Bu holatda chapdagi 61 bit o‘ng tomonga ko‘chiriladi (left shift operation).

- S-box yordamida kalitning yuqori 4 bitiga chiziqsiz almashtirish (substitution) qo‘llaniladi.
- Round raqamiga asoslanib, kalitning oxirgi bitlari yangilanadi.

Har bir raundda yangi kalit yuqorida keltirilgan tartibda hosil qilinadi va K registri yangilanadi. Bu jarayon key schedule deb ataladi va algoritm bardoshliligini oshirishda muhim ro‘l o‘ynaydi. Har bir raundda yangi kalitning hosil bo‘lishi, algoritmini va uning tahlil qilish jarayonini murakkablashtiradi.

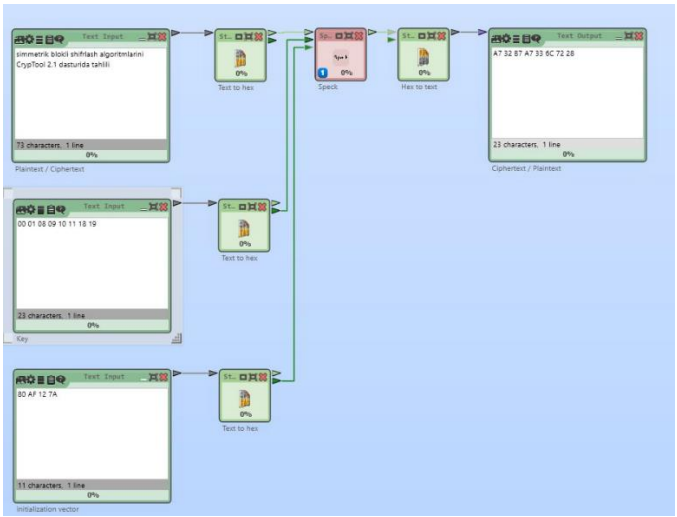
Natijalar. PRESENT shifrlash algoritmini CrypTool 2.1 dasturi ta’minot muhitida ishlatib ko‘rildi va algoritmni solishtirish uchun ikkinchi algoritm sifatida Speck blokli shifrlash algoritmi tanlab olindi va quyidagi natijalar olindi. PRESENT shifrlash algoritmi uchun quyidagi ochiq matn kiritildi. Algoritmni ishlash sxemasi 3-rasmda keltirildi.



3-rasm. PRESENT shifrlash algoritmini dasturiy ta’minotda ishlash jarayoni

3-rasmda PRESENT shifrlash algoritmida ochiq matn sifatida “simmetrik blokli shifrlash algoritmlarini CrypTool 2.1 dasturida tahlili” olindi va Text Output da shifrmatn chiqdi.

Algortimni imkoniyatlarini solishtirish maqsadida SPECK yengil vaznli shifrlash algoritmi tanlab olindi. SPECK - bu 2013-yilda AQSh Milliy Xavfsizlik Agentligi (NSA) tomonidan taklif qilingan mashhur yengil shifrlash algoritmidir. Uning maqsadi cheklangan qurilmalarda xavfsizlikni ta’minlashdir.



4-rasm. SPECK shifrlash algoritmini dasturiy ta’minotda ishlash jarayoni

4-rasmda SPECK shifrlash algoritmida ochiq matn sifatida “simmetrik blokli shifrlash algoritmlarini CrypTool 2.1 dasturida tahlili” olindi va Text Outputda shifrmatn chiqdi.

Olingan natijalar asosida tahliliy jadval hosil bo‘ldi. 3-jadvalda PRESENT va SPECK shifrlash algoritmlarining natijalari qayd qilindi. Jadvalda algoritmlarning kiruvchi ma’lumotlari (plaintext, key, va initialization vector) va ularning chiqish natijalari (ciphertext va qayta ochilgan plaintext) ko‘rsatiladi.

3-jadval. Algoritmlarning o‘zaro xususiyatlari

Xususiyat	**PRESENT**	**SPECK**
Ochiq matn	Simmetrik blokli shifrlash algoritmlarini CrypTool 2.1 dasturida tahlili	Simmetrik blokli shifrlash algoritmlarini CrypTool 2.1 dasturida tahlili
Kalit	Tasodifiy (Random Key)	00 01 08 09 10 11 18 19
IV (initialization Vector)	Tasodifiy (Random IV)	80 AF 12 7A
Shifr matn	67 9C A2 76 3F 9D 13 32 DB B3 50 A6	A7 32 B7 A7 33 6C 72 28

IoT (Internet of Things) qurilmalari uchun shifrlash algoritmlarini tanlashda ularning energiya samaradorligi muhim ahamiyatga ega. 4-jadvalda PRESENT va SPECK shifrlash algoritmlarining IoT qurilmalari uchun energiya samaradorligini solishtirma tahlili keltirildi.

4-jadval. Simmetrik shifrlash algoritmlarni energiya samaradorligi bo‘yicha solishtirma jadvali

Xususiyat	**PRESENT**	**SPECK**
Blok hajmi	64 bit	32, 64, 128 bit
Kalit uzunligi	80, 128 bit	64, 96, 128 bit
Shifrlash davrlar soni	31	22
Shifrlash uchun energiya	4.5 µJ	2.5 µJ
Resurs talabi	Kam	Juda kam
Xavfsizlik darajasi	Yuqori	O‘rtacha-yuqori
Tezlik	Dasturiy muhitda sekinroq	Dasturiy muhitda tezroq

Xulosa sifatida shuni aytish joizki yengil vaznli kriptografik algoritmlar IoT qurilmalari uchun samarali shifrlash, xavfsizlikni ta’minlash imkoniyatlarini taqdim etadi. PRESENT yengil vaznli kriptografik algoritmi ham shular jumlasidandir. IoT qurilmalarida energiya sarfini kamaytiruvchi yengil vaznli kriptografik algoritmlarga ehtiyoj mavjud bu esa yengil vaznli kriptografik algoritmni ishlash samaradorligini yanada takomillashtirish muammolari mavjudligini ko‘rsatadi. Xavfsizlik darajasi yuqori talab qilinadigan IoT qurilmalari (sog‘liqni saqlash qurilmalari, sanoat IoT) uchun mos yengil vaznli shifrlash algoritmining ishlash samaradorligini oshirish muhim vazifa qilib belgilandi. Qiyosiy tahlil natijasi sifatida quyidagilar keltirildi. Jumladan, apparat resurslari cheklangan bo‘lsa PRESENT algoritmi yaxshi tanlov hisoblanadi. Kam quvvatli IoT qurilmalari uchun mos. Energiya samaradorligi va tezlik bo‘lsa, SPECK shifrlash algoritmini tanlash afzalroq. Agar xavfsizlik va apparat resurslarining minimal bo‘lishi talab qilinsa PRESENT yaxshi tanlovdir. Tezlikni oshirish vaqtni kamaytish uchun iteratsiyalar sonini 28 ta deb qabul qilish kechikishlarni optimallashtirish va bunga parallel ravishda energiya sarfini kamaytirishga olib keladi. Ushbu berilgan taklif amaliy natijalari tadqiqotni keyingi bosqichida amalga oshirilishi vazifa qilib belgilandi.

Foydalanilgan adabiyotlar

1. Zscaler ThreatLabz. (2024, November 22). New ThreatLabz report: Mobile remains the top threat vector with 111% spyware growth. Zscaler.
2. Rana, M.& Mamun, Q & Islam, R. Balancing Security and Efficiency: A Power Consumption Analysis of a Lightweight Block Cipher. Electronics 2024, 13, 4325. https://doi.org/10.3390/electronics13214325
3. Christophe De Canniere & Orr Dunkelman & Miroslav Knezevic., KATAN and KTANTAN-a family of small and efficient hardware-oriented block ciphers., Cryptographic Hardware and Embedded Systems-CHES

2009., Springer LNCS, vol. 5747, 2009, pp. 272–288.
4. J. Borghoff., PRINCE–a low-latency block cipher for pervasive computing applications., Advances in Cryptology–ASIACRYPT., Springer LNCS, vol. 7658, 2012, pp. 208–225.
5. Ray Beaulieu & Douglas Shors, Jason Smith & StefanTreatman Clark, Bryan Weeks & Louis Wingers., The SIMON and SPECK families of lightweight block ciphers., IACR Cryptology ePrint Archive (2013).
6. Deukjo Hong& Jaechul Sung, Seokhie Hong& Jongin Lim&Sangjin Lee., HIGHT: A new block cipher suitable for low-resource device., Cryptographic Hardware and Embedded Systems., Springer Berlin Heidelberg, 2006, pp. 46–59.
7. Gaurav Bansod&Nishchal Raval., Implementation of a new lightweight encryption design for embedded security, IEEE Trans. Inf. Forensics Security. 10 (1) (2015) 142–151.
8. G Hatzivasilis&K Fysarakis, I Papaestathi& H Favas., Review of light weight block ciphers., J. Cryptogr. Eng. 8 (2) (2017) 141–184.
9. Dixit R& Kumar L&Verma S, Gupta K&Jain S., An overview of lightweight cipher., CEUR Workshop Proceedings. https://doi.org/10.1016/j.aci.2018.
10. Bogdanov A&Knudsen L. Leander G& Paar "PRESENT: An ultra-lightweight block cipher"., In Workshop on Cryptographic Hardware and Embedded Systems (pp. 450-466). Springer, Berlin, Heidelberg.
11. Fernando M.& Mahmud S.& Wang S., Lightweight encryption for IoT applications: A comprehensive review., Discover Internet of Things, 3(1), 100100. https://doi.org/10.1016/j.discint.2023.100100 .
12. Qozoqova T.Q. & Shamshiyeva B.M., Applying the CryptoSMT software tool to symmetric block encryption algorithms. pp-750-754
13. Qozoqova T.Q. Teaching cryptanalysis of classic encryption methods using modern tools. «Инновации, знания, опыт – векторы образовательных треков» КНИГА I
14. https://www.zscaler.com/blogs/security-research/new-threatlabz-report-mobile-remains-top-threat-vector-111-spyware-growth