YENGIL VAZNLI BLOKLI SHIFRLASH ALGORITMLARINING QIYOSIY TAHLILI

Tursunov Otabek Odiljon o‘g‘li
Muhammad al-Xorazmiy nomidagi
TATU katta o‘qituvchisi
o.o.tursunov@gmail.com
Daminov Akmal Abdurasul o‘g‘li
Muhammad al-Xorazmiy nomidagi TATU assistenti
bek16daminov@gmail.com

Annotatsiya: Yengil kriptografiya resurslari cheklangan qurilmalar (xotira, quvvat, qayta ishlash qobiliyati cheklangan), masalan, radiochastotali identifikatsiya teglari, kontaktsiz smart-kartalar va buyumlar interneti (IoT) uchun ishlatiladi. Yengil blokli shifrlashni loyihalash yillar davomida faol tadqiqot mavzusi bo‘lib kelmoqda. Blokli yengil vaznli shifrlar qiyosiy baholanishi keltirilgan.

Kalit so‘zlar: Yengil vaznli blokli shifr, PRESENT, DESL, PRINT, EPCBC, TWINE, PUFFIN, KLEIN, KATAN, LED, LBLOCK, RECTANGLE.

COMPARATIVE ANALYSIS OF LIGHTWEIGHT BLOCK ENCRYPTION ALGORITHMS

Tursunov Otabek Odiljon ugli
Senior Lecturer, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
o.o.tursunov@gmail.com
Daminov Akmal Abdurasul ugli
Senior Assistant, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi
bek16daminov@gmail.com

Abstract: Lightweight cryptography is used for devices with limited resources (limited memory, power, processing power), such as radio frequency identification tags, contactless smart cards, and the Internet of Things (IoT). The design of lightweight block ciphers has been an active research topic for years. A comparative evaluation of lightweight block ciphers is presented.

Keywords: lightweight block cipher, PRESENT, DESL, PRINT, EPCBC, TWINE, PUFFIN, KLEIN, KATAN, LED, LBLOCK, RECTANGLE.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ АЛГОРИТМОВ ЛЁГКОГО БЛОЧНОГО ШИФРОВАНИЯ

Турсунов Отабек Одилжон угли
старший преподаватель ТУИТ
имени Мухаммада ал-Хорезми
o.o.tursunov@gmail.com
Даминов Акмал Абдурасул угли
старший ассистент ТУИТ
имени Мухаммада ал-Хорезми
bek16daminov@gmail.com

Аннотация: Легковесная криптография используется для устройств с ограниченными ресурсами (ограниченная память, энергопотребление, вычислительная мощность), таких как метки радиочастотной идентификации, бесконтактные смарт-карты и Интернет вещей (IoT). Разработка легковесных блочных шифров является активной темой исследований на протяжении многих лет. В данной работе представлена сравнительная оценка легковесных блочных шифров.

Ключевые слова: лёгкий блочный шифр, PRESENT, DESL, PRINT, EPCBC, TWINE, PUFFIN, KLEIN, KATAN, LED, LBLOCK, RECTANGLE.

1. KIRISH

Yengil simmetrik blokli shifr algoritmlar XOR, AND, 4x4 bitli S-blok kabi asosiy operatsiyalarga tayanadi, bu esa xavfsizlikning yetarli darajada ta’minlanishi uchun talab qilinadigan raundlar sonining oshishiga olib keladi. Yengil simmetrik blokli shifrlash algoritmlari ko‘pincha xotira talablari tufayli kalit jadvalini juda soda holda shakllantiradi [1].

Resurslari chegaralangan qurilmalar (xotirasi cheklangan, quvvati cheklangan va qayta ishlash qobiliyati past bo‘lgan qurilmalar), masalan, radiochastotali identifikatsiya (RFID) teglari, kontaktsiz smart-kartalar, simsiz sensor tarmoqlari, narsalar interneti (IoT) hozirda ko‘plab sohalarda qo‘llanilmoqda. Xavfsizlik uchun ularga yengil kriptografik algoritmlar kerak.

Kriptografik algoritmlarni baholash energiya sarfi, tezlik va xavfsizlikka asoslanadi. Yengil simmetrik blokli shifrlash algoritmlarida energiya sarfini

minimallashtirish asosiy omil hisoblanadi. Shuning uchun energiya sarfi, tezlik va xavfsizlik bilan birgalikda ishlatiladi.

PRINT, LED va KTANTAN kabi algoritmlar apparat nuqtayi nazaridan juda arzon hisoblanadi. DESL, PRESENT, KATAN, EPCBC, LED, LBLOCK va RECTANGLE kabi algoritmlar qurilmada faqat shifrlash funksiyalaridan foydalanadi, TWINE, Puffin va KLEIN kabi boshqa algoritmlar esa ham shifrlash, ham deshifrlash funksiyalaridan foydalanadi.

Shu sababli, har qanday platformada haqiqatan ham past xarajat va kam energiya sarfi maqsadiga erishadigan blokli shifrlash algoritmlarini o‘zaro solishtirish qiyin. Natijada, bu algoritmlar uchun xarajat, energiya sarfi, tezlik va xavfsizlik o‘rtasida muvozanat o‘rnatish murakkab hisoblanadi.

Past tan narxga erishish uchun seriyalashtirilgan ishlab chiqarish va kichik kalit o‘lchami qo‘llaniladi. Yuqori o‘tkazuvchanlik uchun raundlar soni kam bo‘ladi, yuqori xavfsizlik uchun esa raundlar soni ko‘proq bo‘ladi.

2. METODOLOGIYA VA ADABIYOTLAR TAHLILI (YENGIL VAZNLI BLOKLI SIMMETRIK SHIFRLASH ALGORITMLARI)

Ushbu maqola turli yengil blokli simmetrik shifrlash algoritmlari ko‘rib chiqiladi, hamda ularning qiyosiy tahlili beriladi. Oxirgi qismda maqolaga yakuniy xulosa keltiriladi.

Turli simmetrik kalitli yengil blokli shifrlash algoritmlari

PRESENT

PRESENT - bu apparatga moslashtirilgan, juda yengil blokli shifrlash algoritmi hisoblanib, u resurs va energiya sarfi cheklovlarini hisobga olib ishlab chiqilgan. U SP TARMOQ (Substitution-Permutation Network) tarmog‘i asosida qurilgan. Uning blok o‘lchami hajmi 64 bit, kalit uzunligi esa 80 yoki 128 bit, jami 31 ta raunddan iborat. Bu yerda S-box 4 bitli bo‘lib, har raundda 16 marta qo‘llaniladi [2].

Har raund quyidagi 3 bosqichdan iborat:

1. *AddRoundKey*: Kalit bilan shifrlangan matn XOR qilinadi.
2. *Substitution*: 4 bitli S-box qo‘llaniladi.
3. *Permutation*: P-layer aralashtirish (permutatsiya) amalga oshiriladi.

PRESENT algoritmida ishlatiladigan S-box quyidagicha: *S(x) = {c, 5, 6, b, 9, 0, a, d, 3, e, f, 8, 4, 7, 1, 2}*

Har raundda raund kaliti (64 bitli) joriy kalitning eng chap (katta) 64 bitidan olinadi va yangilanadi. Yangilash uchun kalit bitlari chapga 61 pozitsiyaga aylantiriladi (rotatsiya). So‘ngra k79, k78, k77 va k76 bitlari S-box orqali o‘tkaziladi. Yakunda, 5 bitli raund hisoblagichi (round-counter) k19, k18, k17, k16 va k15 bilan XOR qilinadi.

PRINT

PRINT shifri integral sxemalarni chop etish uchun mo‘ljallangan. integral sxemalarni chop etish texnologiyasi sxemalarni juda arzon narxda ishlab chiqarish va

moslashtirish imkonini beradi. PRINT algoritmi ham SP TARMOQ tarmoq asosida qurilgan bo‘lib, uning substitutsiya qatlami 16 ta 3 bitli S-boxlardan iborat, permutatsiya qatlami esa chiziqli diffuziyani ta’minlaydi [3].

PRINT shifri 48 yoki 96 bitli blok o‘lchamiga, 80 yoki 160 bitli kalit o‘lchamiga ega bo‘lib, mos ravishda 48 yoki 96 raunddan iborat. Har ikkala PRINT varianti ham doimiy kalitli algoritmlar bo‘lib, har raundda kalitni yangilash talab qilinmaydi. Kalit ikki qismga bo‘linadi: bir qismi shifrlangan matn bilan XOR qilinadi, ikkinchi qismi esa S-boxdan oldin permutatsiya uchun ishlatiladi.

Har raund quyidagi 5 bosqichdan iborat:

1. Kalit bilan shifrlangan matn XOR qilinadi.
2. Shifrlangan matn chiziqli diffuziya yordamida aralashtiriladi.
3. Shifrlangan matnning eng o‘ngdagi 6 biti raund konstantasi bilan XOR qilinadi.
4. Bitlar kalitga bog‘liq permutatsiya orqali o‘zgartiriladi.
5. Shifrlangan matn S-box yordamida aralashtiriladi.

PRINT algoritmida ishlatiladigan S-box quyidagicha: $S(x)=\{0, 1, 3, 6, 7, 4, 5, 2\}$.

EPCBC

EPCBC (Electronic Product Code Encryption) - bu Elektron mahsulot kodini shifrlash uchun ishlab chiqilgan shifrlash algoritmidir. Elektron mahsulot kodlarini identifikatsiyalash uchun 96 bit talab qiladi. PRESENT shifrida kalit o‘lchami 64bit bo‘lgani uchun ikki marta shifrlash zarur bo‘ladi, AES algoritmida esa kalit 128 bit bo‘lib, ayrim bitlar ortiqcha qolib ketadi. Shuning uchun EPCBC algoritmi yaratilgan[4].

EPCBC ikki turga ega:

- EPCBC (48, 96): 48 bitli blok o‘lchamidan, 96 bitli kalitdan, 32 raunddan iborat;
- EPCBC (96, 96): 96 bitli blok o‘lchamidan, 96 bitli kalitdan, 32 raunddan iborat.

Har ikki algoritm ham shifrlash uchun PRESENT shifri tuzilmasidan (PR−48 va PR−96) foydalanadi hamda PRESENT shifridagi S-boxni qo‘llaydi. EPCBC shifri PRESENT shifridan asosan kalit jadvali (key scheduling) jihatidan farq qiladi.

EPCBC (48, 96) uchun kalit jadvali 96 bitli kalitning chap yarmi birinchi round kaliti sifatida olinadi va 8 raundli Feystil tarmog‘idan foydalanadi. Har bir Feystil tarmog‘I PR−96 shifrining 4 raundidan iborat bo‘lib, bunda kalit qo‘shish bosqichi mavjud emas.

EPCBC (96, 96) uchun kalit jadvali: 96 bitli kalitning barchasi birinchi subkalit sifatida ishlatiladi va PR−96 shifrining 32 raundi qo‘llaniladi (kalit qo‘shishsiz), natijada 32 ta round kaliti hosil qilinadi.

DES, DESL, DESX va DESXL

DESL - bu DES algoritmining yengillashtirilgan (lightweight) blokli shifri hisoblanadi. U 64 bitli blok o‘lchamiga, 56 bitli kalit va 16 ta raunddan iborat. Oddiy DESda 8 ta turli S-box ishlatilsa, DESLda bitta (6×4 bitli) S-box 8 marta takroran qo‘llaniladi. Va yana, boshlang‘ich va yakuniy permutatsiyalar olib tashlangan, bu esa apparat resurslari hamda energiya sarfini kamayishiga olib keladi [5].

14	5	7	2	11	8	1	15	0	10	9	4	6	13	12	3
5	0	8	15	14	3	2	12	11	7	6	9	13	4	1	10
4	9	2	14	8	7	13	0	10	12	15	1	5	11	3	6
9	6	15	5	3	8	4	11	7	1	12	2	0	14	10	13

1-rasm. DESL va DESXL shifrlari uchun S-box jadvali

Yuqori xavfsizlik darajasini ta’minlash uchun DESning yana bir varianti — DESX qo‘llaniladi. DESX 184 bitli kalitga ega (k = 56 bit, k1 = 64 bit, k2 = 64 bit) hamda quyidagicha hisoblanadi: $DESX_{k1, k2, k3}(x) = k2 \oplus DES_k(k1 \oplus x)$

DESXL esa DESX’ning yengillashtirilgan versiyasi bo‘lib, 64 bitli blok o‘lchamiga, 184 bitli kalitga ega va 16 raunddan iborat.

TWINE

TWINE juda kichik apparat resurslarida ishlatish uchun mos va o‘rnatilgan dasturiy ta’minotda yaxshi tezlikni ta’minlaydi. TWINE - bu yuqori darajada diffuziyaga ega bloklarni aralashtirish orqali ishlaydigan Type-2 umumlashtirilgan Feystil tarmog‘i asosida qurilgan [6].

TWINE ikki turga ega: *TWINE-80* va *TWINE-128*. Har ikkala algoritmning blok o‘lchami hajmi 64 bit va 36 ta raunddan iborat. Farqi shundaki, TWINE-80 da kalit uzunligi 80 bit, TWINE-128 da esa 128 bit.

Har bir raund quyidagilarni qamrab oladi:

- 4 bitli S-boxlar yordamida *nochiziqli almashtirish (substitution)* qatlami;
- 4 bitli bloklarni permutatsiya qiluvchi *diffuziya qatlami.*

Ushbu raund funksiyasi har ikki kalit uzunligi uchun ham 36 marta takrorlanadi.

TWINE shifrida ishlatiladigan S-box quyidagicha: s(x)={c, 0, f, a, 2, b, 9, 5, 8, 3, d, 7, 1, e, 6, 4}

Shifrlash jarayoni ushbu bosqichlardan iborat:

– 64 bitli blok 4 bitli 16 ta bloklarga bo‘linadi;

– faqat toq indeksli bloklar quyidagicha o‘zgartiriladi: $S(X_{i-1} \oplus RK_i) \oplus X_i$ bu yerda RK_i — i-raunddagi 4 bitli round kaliti;

– Shundan so‘ng barcha bloklar aralashtiriladi.

Kalitni shakllantirish quyidagicha:

– 80 bitli kalit 20 ta 4 bitli bloklarga bo‘linadi;

– birinchi round kaliti uchun 1, 3, 4, 6, 13, 14, 15 va 16-bloklar tanlanadi;

– kalitni yangilanish jarayoni;
  - 1-blok: $(X_1 \oplus S(X_0))$;
  - 4-blok: $(X_4 \oplus S(X_{16}))$;
  - 7 va 19-bloklar raund sanog‘i bilan XOR qilinadi;
– oxirida barcha bloklar 4 blokga chapga siklik siljitiladi.

Puffin

Puffin - bu involyutsion (o‘ziga teskari) SP TARMOQ tarmog‘i asosidagi shifrlash tizimi hisoblanadi. Involyutsion xususiyat shuni anglatadiki, shifrlash va rasshifrlash jarayonlarida bir xil ma’lumot yo‘li ishlatiladi [7].

Puffin oddiy kalit generatsiya algoritmiga ega bo‘lib, u “on-the-fly” (jarayon davomida) round kalitlarni generatsiya qiladi, ya’ni barcha round kalitlarni oldindan saqlashga ehtiyoj yo‘q.

U past apparat murakkabligi, yaxshi tezlikka ega bo‘lib, ASIC (Application Specific Integrated Circuit) va FPGA texnologiyalari uchun mos hisoblanadi.

Puffin shifrining blok o‘lchami 64 bitdan iborat, kalit o‘lchami 128 bit bo‘lib, shifrlash va rasshifrlash uchun 32 ta raund talab etiladi.

Har bir raund quyidagicha 3 bosqichdan iborat:

1. *Substitution (S):* 4 bitli S-box ishlatiladi;
2. *Key addition (K):* bit darajasida XOR amali;
3. *Permutation (P):* P-layer (permutatsiya qatlami).

Shifrlash ushbu formula bo‘yicha amalga oshiriladi: $C = K_{k0}\, \mathrm{P}\{SK_{kr}P\}_{r=1}^{32}$

Rasshifrovkalash quyidagi formula bo‘yicha amalga oshiriladi: $M = K_{Pk32}\, \mathrm{P}\{SK_{Pkr}P\}_{r=31}^{0}$

Puffin shifrida ishlatiladigan S-box: $S(x)=\{d, 7, 3, 2, 9, a, c, 1, f, 4, 5, e, 6, 0, b, 8\}$

Bu S-box shifrlash va deshifrlashda bir xil ishlatiladi.

Kalitni shakllantirish (Shifrlash):

– Har bir raundda P permutatsiyasi qo‘llaniladi;
– 1, 2, 3, 5-bitlar barcha raundlarda teskari qilinadi;
– 2, 5, 6, 8-raundlarda bu qoida qo‘llanilmaydi.

Kalitni shakllantirish (Rasshifrovkalash):

– Har raundda P^{-1} (teskari permutatsiya) ishlatiladi;
– 30, 62, 71, 120bitlar invert qilinadi;
– Biroq 2, 5, 6, 8raundlarda bu o‘zgartirishlar amalga oshirilmaydi.

KATAN va KTANTAN

KATAN juda samarali, apparatga yo‘naltirilgan blokli shifrlash algoritmi bo‘lib, 80 bitli kalitni qabul qiladi va 32, 48 hamda 64 bitli turli blok o‘lchamlarida ishlaydi.

KATAN oilasidagi blokli shifrlar ikki guruhga bo‘linadi:

– birinchi guruh: KATAN, KATAN-32, KATAN-48, KATAN-64;

– ikkinchi guruh: KTANTAN, KTANTAN-32, KTANTAN-48, KTANTAN-64;

KTANTAN algoritmi KATAN ga qaraganda yanada ixcham, lekin faqat qurilma kaliti oldindan o‘rnatilgan holatlarda ishlatiladi. Ikkala algoritm o‘rtasidagi asosiy farq — kalitni shakllantirish mexanizmidadir.

KATAN va KTANTAN algoritmlarida ochiq matn ikki qismga bo‘linadi. Har raundda bir nechta bitlar olinib, ikkita nochiziqli *boolean* funksiyaga kiradi va ularning chiqishi bir bitga chapga siljitiladi. Jami 254 ta raund bajariladi.

KATAN va KTANTAN da ishlatiladigan ikki nochiziqli *boolean* funksiyalar:

$f_a(A) = A[x_1] \oplus A[x_2] \oplus (A[x_3] * A[x_4]) \oplus (A[x_5] * IR) \oplus k_a$

$f_b(B) = B[y_1] \oplus B[y_2] \oplus (B[y_3] * B[y_4]) \oplus (B[y_5] * B[y_6]) \oplus k_b$

Bu yerda x_i va y_j — A va B qismlaridan tanlangan bitlar, *IR* — raund funksiyasining tartibsiz yangilanishi.

KATAN uchun kalitni shakllantirish (key schedule)

Kalit LFSR ga yuklanadi. Round kaliti quyidagicha olinadi: $k_a \parallel k_b = k_{2*i} \parallel k_{2*i+1}$ bu yerda:

$$k_i = \begin{cases} K_i & for\ i = 0 \dots 79 \\ k_{i-80} \oplus k_{i-61} \oplus k_{i-50} \oplus k_{i-13} & aks\ holda \end{cases}$$

Oxirida LFSR ikki marta yangilanadi (clocked).

LED

LED (Light Encryption Device) - bu dasturiy ta’minotda ham yaxshi ishlash ko‘rsatkichiga ega bo‘lgan, muvozanatli tezlikka ega 64 bitli blokli shifridir. U 64, 80, 96 va 128 bitli kalit o‘lchamlarini qo‘llab-quvvatlaydi. LED shifrida PRESENT algoritmining S-box qismi ishlatiladi.

Shifrlash jarayoni

64 bitli ochiq matn (16 ta 4 bitli qism blok) kvadrat massiv ko‘rinishida joylashtiriladi. Raund funksiyasi quyidagicha ishlaydi: 64 bitli kalit uchun s = 8, boshqa kalitlar uchun s = 12).

Har bir raund quyidagi boshqichlardan iborat:

1. *AddRoundKey* – kalit bilan XOR amali bajariladi
2. *STEP* (4 bosqichdan iborat):
   - *AddConstants* – raund konstantalari bilan XOR;
   - *SubCells* – har bir qism blok PRESENT *S-box* orqali almashtiriladi;
   - *ShiftRows* – i-qatordagi elementlar i pozitsiyaga chapga siljitiladi;
   - *MixColumnsSerial* – ustun vektorlari qayta aralashtiriladi.

Kalitni shakllantirish (Key Scheduling)

64 bitli kalit: barcha round kalitlar bir xil bo‘ladi.

128 bitli kalit: round kalitlar navbat bilan chap va o‘ng qismlarga teng qilib olinadi.

LBLOCK

LBLOCK apparat muhitlarida ham, dasturiy platformalarda ham samarali amalga oshiriladigan blokli shifrlash algoritmidir. Uning blok o‘lchami 64 bit, kalit o‘lchami 80 bit bo‘lib, 32 ta raunddan iborat. LBLOCK Feystil tarmog‘i asosida qurilgan.

LBLOCK dizayni S-box qatlami va P-permutatsiya qatlamidan iborat. Algoritmda 10 ta turli 4×4 bitli S-box ishlatiladi: ulardan 8 tasi shifrlashda, qolgan 2 tasi esa kalitni shakllantirishda qo‘llaniladi.

S_0	14	9	15	0	13	4	10	11	1	2	8	3	7	6	12	5
S_1	4	11	14	9	15	13	0	10	7	12	5	6	2	8	1	3
S_2	1	14	7	12	15	13	0	6	11	5	9	3	2	4	8	10
S_3	7	6	8	11	0	15	3	14	9	10	12	13	5	2	4	1
S_4	14	5	15	0	7	2	12	13	1	8	4	9	11	10	6	3
S_5	2	13	11	12	15	14	0	9	7	10	6	3	1	8	4	5
S_6	11	9	4	14	0	15	10	13	6	12	5	7	3	8	1	2
S_7	13	10	15	0	14	4	9	11	2	1	8	3	7	5	12	6
S_8	8	7	14	5	15	13	0	6	11	12	9	10	2	4	1	3
S_9	11	5	15	0	7	2	9	13	4	8	1	12	14	10	3	6

2-rasm. LBLOCK shifri uchun S-bix jadvali

Shifrlash algoritmi

Agar $M = X_1 \,||\, X_0$ 64 bitli ochiq matn bo‘lsa, shifrlash quyidagicha amalga oshiriladi: $X_i = F(X_{i-1}, K_{i-1}) \oplus (X_{i-2} <<< 8)$, *for* $i = 2 \ldots 33$

Natijaviy 64 bitli shifr matn: $C = X_{32} \,||\, X_{33}$

Bu yerda F (raund funksiyasi) quyidagicha: $F(X, K_i) = P(S(X \oplus K_i))$

Rasshifrovkalash algoritmi

Agar $C = X_{32} \,||\, X33$ bo‘lsa, rasshifrovkalash:

$X_j = F(X_{j+1}, K_{j+1}) \oplus (X_{j+2} >>> 8)$, *for* $i = 31 \ldots 0$

Natijada 64 bitli ochiq matn olinadi: $M = X_1 \,||\, X_0$

Kalitni generatsiyalash (Key Scheduling)

– 80 bitli kalit $K = k_{79}k_{78} \ldots k_0$

– dastlabki round kaliti K_1 eng chap 32 bit;

– keyin kalit 31 marta yangilanadi;

- 29 marta chapga siljitiladi; $k_{79}k_{78}k_{77}k_{76}$ va $k_{75}k_{74}k_{73}k_{72}$ bitlar S-boxdan o‘tkaziladi; $k_{50}k_{49}k_{48}k_{47}$ bitlar raund hisoblagichi bilan XOR qilinadi;

– yangilangan kalitning chap 32 biti K_2 va keyingi round kalitlar hosil qilinadi.

LBLOCK yengil kriptografiya uchun optimallashtirilgan va resurslari cheklangan tizimlarda samaraliroq ishlashga mo‘ljallangan.

RECTANGLE

RECTANGLE - bu bit-slice (bit bo‘laklashga asoslangan) ultra-yengil blok shifrlash algoritmi, apparatda juda kichik resurs (area) talab qiladi va dasturiy muhitda ham yuqori tezlikka ega. RECTANGLE SP TARMOQ asosida qurilgan.

S-qatlam 16 ta 4 bitli S-boxlardan iborat, P-qatlam esa 3 ta aylantirish (rotation) operatsiyasidan tashkil topgan.

RECTANGLE algoritmi 64 bitli blok o‘lchamga ega, kalit uzunligi 80 yoki 128 bit bo‘lib, 25 ta raunddan iborat. Kalit (n = 20 / 32) va ochiq matn (n = 16) 4 × n o‘lchamli to‘rtburchak (rectangular) bit massiv ko‘rinishida ifodalanadi.

Har raund 3 bosqichdan iborat:

1. *AddRoundKey* – bit darajasida XOR amali;
2. *SubColumn* – har bir ustundagi 4 bit S-box orqali almashtiriladi;
3. *ShiftRow*, 0-qator siljitilmaydi, 1-qator chapga 1 bit siljitiladi, 2-qator chapga 12 bit siljitiladi, 3-qator chapga 13 bit siljitiladi.

RECTANGLE S-box quyidagi ko ‘rinishga ega:

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

Kalitni generatsiyasi (Key scheduling)

Har raundda kalit 64 bitning eng o‘ngdagi 16 ustunidan olinadi va quyidagicha yangilanadi:

– 0 ustunga S-box qo‘llanadi;
– qatorlar chapga quyidagicha siljitiladi:
  - qator 0: 7 bit, qator 1: 9 bit, qator 2: 11 bit, qator 3: 13 bit;
– eng o‘ngdagi 5 bitga raund konstantasi (RC) XOR qilinadi.

RECTANGLE yengil kriptografiya uchun optimallashtirilgan bo‘lib, ayniqsa resurslari chegaralangan qurilmalar uchun mos hisoblanadi.

3. QIYOSIY TAHLIL NATIJALARI

Turli yengil blok shifrlash algoritmlari 1-jadvalda kalit o‘lchami, blok o‘lchami, funksiyasi, arxitekturasi, tuzilmasi, har blok uchun sikllar soni, o‘tkazuvchanlik (throughput) va resurs talabi (Gate Equivalents) bo‘yicha taqqoslangan.

Ikki turdagi arxitektura mavjud: *serialized (ketma-ket)* va *round based (raund asosida)*.

Serialashtirilgan arxitektura past resurs talabi (Gate Equivalents) uchun ishlatiladi; bu holda ma’lumotning qism bloki o‘lchami 4 bitga teng bo‘ladi.

Round based arxitektura esa yuqori o‘tkazuvchanlik uchun ishlatiladi; bu holatda ma’lumot qism bloki o‘lchami blok o‘lchamiga teng bo‘ladi.

1-jadval.

Yengil vaznli simmetrik blokli shifrlash algoritmlarining qiyosiy tahlili

Shifr algoritm	Tarmoq turi	Blok o‘lcha-mi	Kalit o‘lchami	Raundlar soni	Resurs (GEs)	Cycles /Block	Tezlik (b/s)

PRINT-48*	SP tarmoq	48	80	48	403	769	6.24
LED-64*	SP tarmoq	64	64	32	685	1249	5.1
KTANTAN-32*	LFSR	32	80	254	459	254	12.5
PRESENT-80	SP tarmoq	64	80	32	1027	520	12.6
EPCBC-48	SP tarmoq	48	96	32	1011	393	12.19
DESXL	Feystil	64	184	16	2635	150	5.56
TWINE-80	Feystil	64	80	36	1500	37	180
Puffin	SP tarmoq	64	128	32	2579	32	194
KLEIN-64	SP tarmoq	64	64	12	2475	13	493.0
KLEIN-64	SP tarmoq	64	64	12	1219	208	31
KATAN-32	LFSR	32	80	254	808	256	13
LED-64	SP tarmoq	64	64	32	967	1249	5
LBlock	Feystil	64	80	32	1320	32	201
REC-TANGLE-80	SP tarmoq	64	80	25	1470	27	247

4. XULOSA

Yengil vaznli blokli shifrlarni qurishda asosan uch xil tarmoq mavjud:

- Substitution-Permutation Network;
- Feystil tarmog‘i;
- LFSR (Linear Feedback Shift Register).

SP TARMOQ tarmog‘i S-box orqali almashtirish (substitution) va P-qatlam orqali aralashtirishdan (permutatsiyadan) foydalanadi. Feystil tarmog‘i esa XOR va chap-o‘ng qismlarni almashtirishga asoslanadi. LFSR esa chiqish biti oldingi holatga bog‘liq bo‘lgan shift registrdan foydalanadi.

PRINT-48, PRINT-96, LED-64, LED-80, LED-96, LED-128, KTANTAN-32, KTANTAN-48 va KTANTAN-64 kabi algoritmlar o ‘zgarmas kalitli (fixed key, hardwired) hisoblanadi va faqat maxsus ilovalarda ishlatiladi.

80 bit kalit va 48 bit blok uchun: PRINT KTANTAN ga qaraganda kamroq maydon egallaydi, lekin KTANTAN ning tezligi yuqoriroq.

80 bit kalit va 64 bit blok uchun: KTANTAN va LED resurs talabi jihatdan bir xil, lekin KTANTAN o‘tkazuvchanlik bo‘yicha ustun.

160 bit kalit uchun PRINT ishlatiladi.

64, 96 yoki 128 bit kalit uchun LED ishlatiladi.

32 bit blok uchun KTANTAN ishlatiladi.

PRESENT, EPCBC, DESL, KATAN, LED, LBLOCK va RECTANGLE algoritmlari faqat shifrlash tomonida ishlaydi (rasshifrovkalash server tomonda amalga oshiriladi).

80 bit kalit uchun LBLOCK maydon jihatdan LED, PRESENT, KATAN va RECTANGLE dan kichikroq, lekin tezlik bo‘yicha KATAN ustunroq hisoblanadi (LBLOCK, LED, PRESENT va RECTANGLE ga nisbatan).

Umuman olganda, yengil kriptografiyada **resurs talabi (area)** va **tezlik (throughput)** o‘rtasida kuchli kompromiss mavjud bo‘lib, har bir algoritm turli apparat va dasturiy ehtiyojlarga moslashtirilgan.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

1. Xudoyqulov Z.T., Rahmatullayev I.R. Yengil vaznli kriptografik algoritmlarda qo‘llanilgan chiziqsiz akslantirish funksiyalarining tahlili // International Journal of Theoretical and Applied Issues of Digital Technologies. – 2024. – Vol. 7, №2. – B. 51–58.

2. Bogdanov A., Knudsen L.R., Leander G., Paar C., Poschmann A., Robshaw M.J.B., Seurin Y., Vikkelsoe C. PRESENT: an ultra-lightweight block cipher // Proceedings of the Cryptographic Hardware and Embedded Systems Conference (CHES 2007). – Springer, 2007. – LNCS 4727. – P. 450–466.

3. Knudsen L.R., Robshaw M.J.B., Leander G., Poschmann A. PRINTcipher: a block cipher designed for IC-printing applications // Cryptographic Hardware and Embedded Systems – CHES 2010. – Springer, 2010. – LNCS 6225. – P. 16–31.

4. Yap H., Khoo K., Poschmann A., Henricksen M. EPCBC block cipher for electronic product code encryption // Cryptology and Network Security. – Springer, 2011. – LNCS 7092. – P. 76–97.

5. Paar C., Leander G., Poschmann A., Schramm K. New lightweight DES-based variants for fast software encryption // Fast Software Encryption Conference Proceedings. – Springer, 2007. – LNCS 4593. – P. 1–18.

6. Suzaki T., Minematsu K., Morioka S., Kobayashi E. TWINE: lightweight and versatile block cipher // Proceedings of the Lightweight Cryptography Workshop (LC 2011). – 2011.

7. Cheng H., Heys H.M., Wang C. Puffin: compact block cipher aimed at embedded digital platforms // 11th EUROMICRO Conference on Digital System Design: Architectures, Methods and Tools (DSD 2008). – IEEE, 2008. – P. 383–390.

8. Singh M.P., Kumar P., Kushwaha P.K. A survey of lightweight block cipher algorithms // International Journal of Computer Applications. – 2014. – Vol. 96, №17. – P. 1–6.