UO‘K 004.056.55:004.89:519.2

S-AES RAUND KALITLARI KRIPTOTAHLILIGA SVM GIPERPARAMETRLARINI OPTIMALLASHTIRISH ORQALI TASNIFLASH YONDASHUVI

Baxtiyor Fayziyevich ABDURAXIMOV
professor
Fizika-matematika fanlari doktori
Mirzo Ulug‘bek nomidagi O‘zbekiston milliy universiteti
Toshkent, O‘zbekiston
a_bakhtiyor@mail.ru
Javohir Rustamovich ABDURAZZOQOV
dotsent
Toshkent xalqaro universiteti
Toshkent, O‘zbekiston
javohirjon.1992@gmail.com
Ilhom Mardonaqulovich BOYQUZIYEV
dotsent
Muhammad al-Xorazmiy nomidagi
Toshkent axborot texnologiyalari universiteti
Toshkent, O‘zbekiston
salyut2017@gmail.com

Annotatsiya

Ushbu maqolada S-AES algoritmi misolida raund kalit bitlarini aniqlash masalasi o‘rganildi. Ma’lumotlar to‘plami turli kalitlar, ochiq matnlar va hosil bo‘lgan shifrmatnlar asosida shakllantirildi. Tasniflash jarayonida SVM (Support Vector Machine) usuli qo‘llanilib, Optuna dasturiy uskunasi yordamida uning giperparametrlari optimallashtirildi.

Tayanch so‘zlar: S-AES, SVM, simmetrik shifrlash algoritmlari, optuna, mashinaviy o‘qitish, raund kalitlari.

ПОДХОД К КЛАССИФИКАЦИИ ПРИ КРИПТОАНАЛИЗЕ РАУНДОВЫХ КЛЮЧЕЙ S-AES НА ОСНОВЕ ОПТИМИЗАЦИИ ГИПЕРПАРАМЕТРОВ SVM

Бахтиёр Файзиевич АБДУРАХИМОВ
профессор
Доктор физико-математических наук
Национальный университет Узбекистана имени Мирзо Улугбека
Ташкент, Узбекистан
a_bakhtiyor@mail.ru
Жавохир Рустамович АБДУРАЗЗОКОВ
доцент
Ташкентский международный университет
Ташкент, Узбекистан
javohirjon.1992@gmail.com
Илхом Мардонакулович БОЙКУЗИЕВ

доцент
Ташкентский университет информационных технологий
имени Мухаммада аль-Хоразмий
salyut2017@gmail.com

Аннотация

В данном статье на примере алгоритма S-AES рассмотрена задача определения битов раундовых ключей. Набор данных был сформирован на основе различных ключей, открытых текстов и соответствующих шифртекстов. Для классификации применён метод SVM, гиперпараметры которого оптимизировались с помощью программного инструмента Optuna.

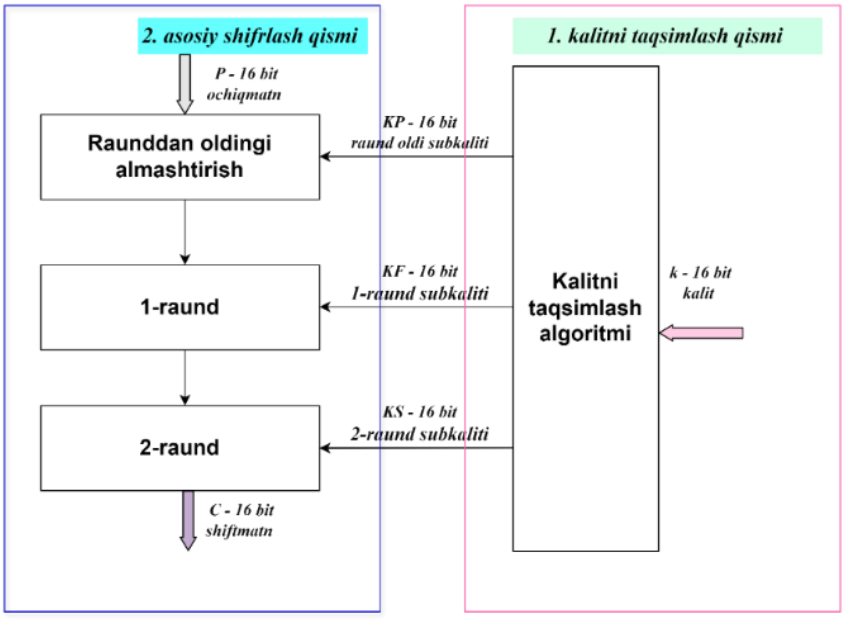
Ключевые слова: S-AES, SVM, симметричные алгоритмы шифрования, Optuna, машинное обучение, раундовые ключи.

Zamonaviy kriptologiyada sun’iy intellekt texnologiyalarining rivojlanishi blokli shifrlash algoritmlarning xavfsizligini ta’minlash borasidagi masalalarni murakkablashtirmoqda. Ayniqsa soddalashtirilgan blokli shifrlarning xavfsizligini tahlil qilishda chuqur o‘qitish usullarini qo‘llash dolzarb mavzuga aylanmoqda. Soddalashtirilgan blokli shifrlar, cheklangan resurslarga platformalar va buyumlar interneti (IoT) qurilmalarida keng qo‘llaniladigan algoritmlardir. Soddalashtirilgan blokli shifrlash algoritmlari qurilmalar uchun kam quvvat talab qilishi bilan birga tezlik tomonlama ustun sanaladi. Kriptotahlilda chuqur o‘qitish asosidagi usullar paydo bo‘lishi ushbu algoritmlarning xavfsizligida yangi tahdidlarni vujudga keltirmoqda. Oxirgi yillarda olib borilayotgan tadqiqotlar chuqur o‘rganish usullarining soddalashtirilgan blokli shifrlar ustida samarali qo‘llanilishi mumkinligini ko‘rsatdi. Jumladan 2020-yilda Jaewoo So tadqiqot ishida chuqur o‘qitish usulini Simon va Speck [1] kabi soddalashtirilgan blokli shifrlar uchun qo‘llagan holda, ularning kalit bitlarini muvaffaqiyatli tikladi, bu usullar ma’lum bir chekli kalit maydonida ishlatilganda samarali bo‘lishini isbotladi [2]. 2020-yilda Aayush Jain va boshqalar soddalashtirilgan PRESENT blokli shifrining shifr ma’lumotlarini, tasodifiy ma’lumotlardan farqlashni chuqur o‘qitishga asoslangan differensial kriptotahlildan foydalangan holda isbotlangan [3]. 2023-yilda Hyunji Kim va boshqalar tadqiqoti esa, chuqur o‘qitish yordamida uning

giperparametrlarini sezilarli darajada kamaytirish va kalit bitini tasniflash aniqligini oshirish orqali mazkur yondashuvni yanada takomillashtirdi [4].

Soddalashtirilgan AES (S-AES). S-AES Santa Klara universiteti professori Edvard Shefer tomonidan ishlab chiqilgan. Mazkur algoritm o‘quvchilarga kichik sonli bitli shifr bloklari va kalitlardan foydalangan holda AES tuzilishini o‘rganishga yordam berish uchun mo‘ljallangan ta’lim vositasidir. Shifrlash jararayonida S-AES 16 bitli ochiq matn va 16 bitli kalitlarni kiritgan holda 16 bitli shifrlangan matnni yaratadi; razshifrovka jarayonida S-AES 16 bitli shifrlangan matnni oladi va 16 bitli kalitdan foydalangan holda 16 bitli ochiq matnni yaratadi [5]. Ushbu jarayon 1-rasmda ko‘rsatilgan. S-AESda uchta raund kalitlari mavjud va *KP*, *KF* va *KS* bilan ifodalanadi [6].

Ma’lumotlarni o‘qishga tayyorlash tadqiqotning muhim qismi hisoblanib, dastlab matritsa ko‘rinishida (1) keltirilgan tasodifiy N ta elementdan iborat K_N to‘plamini tuzamiz. Matritsaning har bir satri kalitni, ustunlar esa kalitning bitlarini ifodalaydi, n esa S-AES blok shifrining kalit uzunligi bo‘lib 16 ga teng. Shunday qilib, $k_{i,j}$ i-kalitdagi j-kalit bitidir. Keyingi qadamda (2) ko‘rsatilganidek, tasodifiy ravishda N ta ochiq matn P_N ni yaratib, avval yaratilgan K_N kalitlari yordamida S-AES shifrlash algoritmiga kiritilib shifmatn hosil qilinadi [7].



1-rasm. *S-AES* shifrlash algoritmi umumiy shifrlash jarayoni.

Tajribalar S-AESning kalit bitlarini tasniflashda turli mashinani o‘qitish usullari va uning parametrlari har bir kalit bitini tasniflashda turlicha aniqlik qiymatlarini ko‘rsatdi. Demak, bunga asoslanib S-AESning kalit bitlarini tasniflashda mashinani o‘qitish usuli bilan birga uning parametrlarini ham optimal tanlash muammosi mavjudligini ko‘rish mumkin.

Mashinaga raund kalitlarini o‘qitish uchun ma’lumotlarni tayyorlash. Ma’lumotlarni o‘qishga tayyorlash N ta elementdan iborat K_N to‘plami elementlarini tasodifiy tanlagan holda tuzamiz (1), (2), (3). Matritsaning satri kalitni, ustunlar kalitning bitlarini ifodalab, n esa *S-AES* shifrining kalit uzunligini bildirib 16 ga teng. Bunda, $k_{i,j}$ i-kalitdagi j-kalit bitidir. Quyida o‘quv tanlanma (O‘T) sifatida tanlab olingan S-AES qismlari berilgan.

$$K_N = \begin{bmatrix} k_{1,1} & k_{1,2} & \cdots & k_{1,n} \\ k_{2,1} & k_{2,2} & \cdots & k_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ k_{N,1} & k_{N,2} & \cdots & k_{N,n} \end{bmatrix} \quad (1) \qquad P_N = \begin{bmatrix} p_{1,1} & p_{1,2} & \cdots & p_{1,n} \\ p_{2,1} & p_{2,2} & \cdots & p_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ p_{N,1} & p_{N,2} & \cdots & p_{N,n} \end{bmatrix} \quad (2)$$

$$C_N = \begin{bmatrix} c_{1,1} & c_{1,2} & \cdots & c_{1,n} \\ c_{2,1} & c_{2,2} & \cdots & c_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{N,1} & c_{N,2} & \cdots & c_{N,n} \end{bmatrix} \quad (3)$$

Ushbu O‘Tlar uchun ochiq matn sifatida 2 ta p_1 = 1000100010001000 va p_2 = 1100110011001100 lar 16 bitdan iborat ochiq matnlar tanlandi. Tanlangan p_1 va p_2 larni raund funksiyalarga bir xil subkalitlar *KP=16 bit, KF=16 bit, KS=16bit* bilan dastlab p_1 bilan shundan so‘ng p_2 bilan shifrlangan ma’lumotlar c_1 va c_2 hosil qilindi. Hosil bo‘lgan c_1 va c_2 shifrmatnlar to‘plamiga *S-AES* ning raund funksiyasining o‘n oltilikdagi nochiziq almashtirish qiymatlari S_b*={9,4,A,B,D,1,8,5,6,2,0,3,C,E,F,7}* ning binar qiymatda O‘Tlarga qo‘shildi. Ushbu jarayonlar orqali raund kalitlarini tasniflash uchun S_{T_1} (4), S_{T_2} (5), S_{T_3} (6) O‘Tlar shakllantirildi. Bunda S_{T_1} (4), raunddan oldingi *KP* subkalit bitlari, S_{T_2} (5)

birinchi raund uchun *KF* raund kaliti bitlari, S_{T_3} (6) ikkinchi raund uchun *KS* raund kalit bitlarini tasniflash uchun olingan O‘Tdir.

$$S_{T_1} = \begin{bmatrix} cb_{1,1} & cb_{1,2} & \cdots & cb_{1,n} & cs_{1,1} & cs_{1,2} & \cdots & cs_{1,n} & sb_{1,1} & sb_{1,2} & \cdots & sb_{1,m} & kp_{1,1} & kp_{1,2} & \cdots & kp_{1,n} \\ cb_{2,1} & cb_{2,2} & \cdots & cb_{2,n} & cs_{2,1} & cs_{2,2} & \cdots & cs_{2,n} & sb_{2,1} & sb_{2,2} & \cdots & sb_{2,m} & kp_{2,1} & kp_{2,2} & \cdots & kp_{2,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ cb_{N,1} & cb_{N,2} & \cdots & cb_{N,n} & cs_{N,1} & cs_{N,2} & \cdots & cs_{N,n} & sb_{N,1} & sb_{N,2} & \cdots & sb_{N,m} & kp_{N,1} & kp_{N,2} & \cdots & kp_{N,n} \end{bmatrix} \quad (4)$$

$$S_{T_2} = \begin{bmatrix} cb_{1,1} & cb_{1,2} & \cdots & cb_{1,n} & cs_{1,1} & cs_{1,2} & \cdots & cs_{1,n} & sb_{1,1} & sb_{1,2} & \cdots & sb_{1,m} & kf_{1,1} & kf_{1,2} & \cdots & kf_{1,n} \\ cb_{2,1} & cb_{2,2} & \cdots & cb_{2,n} & cs_{2,1} & cs_{2,2} & \cdots & cs_{2,n} & sb_{2,1} & sb_{2,2} & \cdots & sb_{2,m} & kf_{2,1} & kf_{2,2} & \cdots & kf_{2,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ cb_{N,1} & cb_{N,2} & \cdots & cb_{N,n} & cs_{N,1} & cs_{N,2} & \cdots & cs_{N,n} & sb_{N,1} & sb_{N,2} & \cdots & sb_{N,m} & kf_{N,1} & kf_{N,2} & \cdots & kf_{N,n} \end{bmatrix} \quad (5)$$

$$S_{T_3} = \begin{bmatrix} cb_{1,1} & cb_{1,2} & \cdots & cb_{1,n} & cs_{1,1} & cs_{1,2} & \cdots & cs_{1,n} & sb_{1,1} & sb_{1,2} & \cdots & sb_{1,m} & ks_{1,1} & ks_{1,2} & \cdots & ks_{1,n} \\ cb_{2,1} & cb_{2,2} & \cdots & cb_{2,n} & cs_{2,1} & cs_{2,2} & \cdots & cs_{2,n} & sb_{2,1} & sb_{2,2} & \cdots & sb_{2,m} & ks_{2,1} & ks_{2,2} & \cdots & ks_{2,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ cb_{N,1} & cb_{N,2} & \cdots & cb_{N,n} & cs_{N,1} & cs_{N,2} & \cdots & cs_{N,n} & sb_{N,1} & sb_{N,2} & \cdots & sb_{N,m} & ks_{N,1} & ks_{N,2} & \cdots & ks_{N,n} \end{bmatrix} \quad (6)$$

S_{T_1} – *KP* raund kalit bitlari tasniflash O‘Tsi. S_{T_2} - *KF* raund kalit bitlari tasniflash O‘Tsi. S_{T_3} - ikkinchi raundga kiruvchi *KS* raund kalit bitlari tasniflash O‘Tsi. *cb*- p_1 ochiq matn va *KP, KF, KS* raund kalit bilan *S-AES* da hosil qilingan shifrmatn. *cs*- p_2 ochiq matn va *KP, KF, KS* raund kalit bilan *S-AES* da hosil qilingan shifrmatn. *sb- S-AES* raund funksiyasi S blokning doimiy qiymatlari. *N* – O‘Tdagi elementlar soni. *n* – *S-AES*ning blok bitlari uzinligi, 16 ga teng. *m* - *S-AES*ning S blokning doimiy binar qiymatlari uzunligi, 64 ga teng. S_{T_1}, S_{T_2}, S_{T_3} O‘Tda elementlar *N=1280* dan iborat bo‘lib, 1024 ta o‘quv tanlanma va 256 ta nazorat tanlanma qismiga ajratildi.

Binar tasniflash muammolarini yechishda SVM boshqalardan ustun bo‘lganligi sababali, ushbu usulni tanlandi [8-10]. SVMda tasniflash aniqligini oshirish uchun uning *C* parametri, yadro funksiyasi, mavjud bo‘lganda yadro funksiyasi parametrlarini tanlashni foydalanuvchi amalga oshiradi. Mos parametrlarni tanlash esa tajriba yoki boshqa optimallashtirish usullari yordamida bajariladi [11,12].

Ushbu masalani yechishda Optuna giper parametrlarni tanlash dasturiy uskunasidan foydalanildi. Optuna dasturiy uskunasini boshqa shu singari HyperOpt [13] va SMAC [14] dasturlari bilan solishtirgan tadqiqotlarda giperparametrlarni optimallashtirish masalalarida yuqori samaradorlik ko‘rsatgan [15, 16].

SVM giperparametrlarini Optuna yordamida optimallashtirish va tanlash masalasini quydagicha bajarildi.

1.Maqsad funksiyasi. SVM ma’lum bir O‘T to‘plami $S = \{(x_1, y_1), \ldots, (x_n, y_n)\}$ uchun har x_i kirish vektori unga mos keluvchi y_i sinfi bo‘lganda quyidagi optimallashtirish masalasini yechish kerak bo‘lsin.

$$\min_{\mathbf{w},b,\xi} \frac{1}{2} \| \mathbf{w} \|^2 + C \sum_{i=1}^{n} \xi_i$$

*2. Shartlar***.** Har bir kiruvchi x_i vektor, chiquvchi y_i ga to‘g‘ri tasniflanishi uchun quydagi shartlar bajarilishi lozim.

$$y_i(\mathbf{w}^T \mathbf{x}_i + b) \geq 1 - \xi_i, \quad \xi_i \geq 0, \quad \forall i = 1, \ldots, n$$

Bu yerda, x_i – ma’lumotlar to‘plamidagi *i*-chi namuna. y_i – x_i ning haqiqiy sinfi. **w** – ajratuvchi sirtning ko‘paytma vektori. *b* – ajratuvchi sirtning ozod hadi (bias), tekislik yoki sirtning o‘rnini aniqlashda ishlatiladigan parametr. ξ_i - *i*-namuna uchun moshlashuvchan o‘zgaruvchisi, noto‘g‘ri tasniflanish darajasi. *C* – noto‘g‘ri tasniflanish bahosining regularizatsiya parametri.

Giperparametrlarni optimallashtirish masalasi. Mashinani o‘qitish modelining ishlashini maksimal darajada yaxshilash maqsadida uning giperparametrlarini sozlash jarayonidir. Modelning test to‘plamidagi aniqligini maksimal qiluvchi giperparametrlar to‘plamini topish. Bu, quyidagi maqsad funksiya orqali amalga oshirildi.

$$\max_{\theta \in \Theta} f\left(\theta; S_{o'quv}, S_{test}\right)$$

Ushbu funksiyada θ – modelning giper parametrlar to‘plami, Θ-giper parametrlarning qidiruv maydoni, $S_{o'quv}$ – O‘T to‘plami va S_{test} – NT to‘plami.

Giper parametrlar va ularning qidiruv maydoni. Giper parametrlar to‘plami $\theta = \{h_1, h_2, \ldots, h_i\}$, har bir h_i giperparametr, Θ_i qidiruv maydonida tanlanishi mumkin bo‘lgan qiymatlarni o‘z ichiga oladi. SVMda quyidagi giperparametrlar va ularning parametrlari maydoni quydagicha tanlandi:

C – regularizatsiya parametri: $C = \left[10^{-3}, 10^{3}\right]$

Y_t – yadro funksiyalari to‘plami. $Y_t = \{y_{ch}, y_k, y_r, y_s\}$, Bunda y_{ch} – chiziqli, y_k –ko‘phadli, y_r – radial asosli, y_s – sigmoidal yadro funksiyalari.

d – daraja ko‘phadli yadro funksiyasi y_k uchun qo‘llaniladi, $d \in \{1, 2, 3, 4, 5\}$.

γ – ko‘phadli y_k, radial asosli y_r, sigmoidal y_s – sigmoidal yadro funksiyalari uchun qo‘llaniluvchi parametr, $\gamma \in \left[10^{-4}, 10^{1}\right]$.

r – ko‘phadli y_k va sigmoidal y_s – yadro funksiyalari uchun qo‘llaniluvchi parametr, $r \in [0, 10]$.

M – optimallashtirishda giper parametrlarni turli qiymatlarda o‘qitish uchun belgilangan sinovlar soni, *M=1000*.

Optuna giperparametrlar to‘plami θ ni berilgan sinovlar soni M marta sinab ko‘rib, nazorat to‘plamida eng yuqori aniqlikka erishuvchi giper parametrlar to‘plamni tanlaydi. Bu optimallashtirish jarayoni, modelning yangi ma’lumotlarga moslashishi, umumlashtiruvchi qobiliyati yaxshilanishi maqsadida amalga oshirildi.

*Model aniqligini baholash***.** Modelning aniqligi M_A, uning y_i' bashorati va sinov namunalaridagi haqiqiy sinfi y_i o‘rtasidagi taqqoslash asosida baholanadi va quyidagicha ifodalanadi.

$$M_A = \frac{1}{N} \sum_{i=1}^{N} I\left(y_i' = y_i\right)$$

Bunda N – jami sinov namunalar soni, va $I(\cdot)$ – indikator funksiyasi bo‘lib, agar prognoz to‘g‘ri bo‘lsa 1, aks holda 0 ga teng bo‘ladi. Ko‘p hollarda modelning aniqligi uning S_{test} nazorat to‘plamidagi jami N ta x_i–kirishlaridan

bashorat qilingan $y_i^{'}$ – qiymati imkon qadar, uning haqiqiy y_i - sinfiga yaqin bo‘lishi bilan yuqori baholanadi.

S-AES algoritmida generatsiya qilingan $S = \{(x_1, y_1), \ldots, (x_n, y_n)\}$ o‘quv tanlanma mavjud. Bunda x_n kiruvchi vektorlar (7) generatsiya qilingan 2 xil shifrmatn bitlari va S blokning qiymatlari orqali y_n ning har bir usulidagi *KP*, *KF* va *KS* bitlarini alohida binar sinfli O‘T shakllangan (8). Shakllantirilgan O‘T, Optuna dasturiy uskunasida SVM uchun tanlangan yuqoridagi θ- giper parametrlar va ularning Θ - qidiruv maydoni qiymatlari asosida *M=1000* ta sinov bilan amalga oshirildi. Optimal giperparametrlar to‘plami *M=1000* ta sinovda kuzatilgan eng katta aniqlik bilan tanlandi.

$$x_n = \begin{bmatrix} cb_{1,1} & cb_{1,2} & \cdots & cb_{1,n} & cs_{1,1} & cs_{1,2} & \cdots & cs_{1,n} & sb_{1,1} & sb_{1,2} & \cdots & sb_{1,m} \\ cb_{2,1} & cb_{2,2} & \cdots & cb_{2,n} & cs_{2,1} & cs_{2,2} & \cdots & cs_{2,n} & sb_{2,1} & sb_{2,2} & \cdots & sb_{2,m} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ cb_{N,1} & cb_{N,2} & \cdots & cb_{N,n} & cs_{N,1} & cs_{N,2} & \cdots & cs_{N,n} & sb_{N,1} & sb_{N,2} & \cdots & sb_{N,m} \end{bmatrix} \quad (7)$$

$$y_n = \begin{bmatrix} kp_{1,1} & kp_{1,2} & \cdots & kp_{1,n} & kf_{1,1} & kf_{1,2} & \cdots & kf_{1,n} & ks_{1,1} & ks_{1,2} & \cdots & ks_{1,n} \\ kp_{2,1} & kp_{2,2} & \cdots & kp_{2,n} & kf_{2,1} & kf_{2,2} & \cdots & kf_{2,n} & ks_{2,1} & ks_{2,2} & \cdots & ks_{2,n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ kp_{N,1} & kp_{N,2} & \cdots & kp_{N,n} & kf_{N,1} & kf_{N,2} & \cdots & kf_{N,n} & ks_{N,1} & ks_{N,2} & \cdots & ks_{N,n} \end{bmatrix} \quad (8)$$

O‘tkazilgan tajribalar asosida olingan tadqiqot natijalari 1-jadvalda keltirilgan. Bunda Y_t – yadro funksiyalari to‘plamni, y_{ch} – chiziqli, y_k –ko‘phadli, y_r – radial asosli, y_s – sigmoidal yadro funksiyalarini bildiradi.

1-jadval

Optuna yordamida S-AES algoritmi raund kalit bitlarini tasniflashda optimallashtirilgan SVM parametrlari

Kalit	C	Y_t	Yadro funksiyalari parametrlari			Eng yuqori aniqlik	Sarf etilgan vaqt (sekund)
			d	γ	r, σ		
kp_1	909,977042	y_r	-	0,000951	-	0,7307	3744
kp_2	741,809773	y_k	-	0,000348	-	0,6923	2548
kp_3	1,544337	y_s	-	0,017831	5,605541	0,6923	3892

kp_4	0,743842	y_r	-	0,166130	-	0,6538	2008
kp_5	183,12256	y_r	-	0,051373	-	0,7115	2768
kp_6	4,569204	y_s	-	0,200912	9,910495	0,8076	2316
kp_7	4,90953	y_s	-	0.437448	0,780156	0,7501	3612
kp_8	0,105297	y_k	4	3,996537	8,341613	0,7307	2256
kp_9	2,113041	y_r	-	0,014773	-	0,7307	2189
kp_{10}	0,065626	y_{ch}	-	-	-	0,7692	2136
kp_{11}	74,613754	y_r	-	0,000798	-	0,6539	3856
kp_{12}	22,584393	y_k	2	0,028741	9,085915	0,6923	3016
kp_{13}	1,639790	y_s	-	0,429163	3,169623	0,6538	2751
kp_{14}	0,130881	y_k	5	0,042843	6,471482	0,7307	2163
kp_{15}	12,292773	y_k	4	0,000146	7,606104	0,7692	3960
kp_{16}	1,667932	y_s	-	0,004939	7,334085	0,7692	2940
kf_1	1,079922	y_r	-	0,035383	-	0,7307	2710
kf_2	529,829905	y_s	-	0,313631	6,417064	0,8846	2653
kf_3	463,658146	y_r	-	0,352861	-	0,6538	3078
kf_4	5,260372	y_r	-	0,268973	-	0,6923	2597
kf_5	7,695986	y_s	-	0,000132	6,509235	0,6538	2164
kf_6	139,452139	y_r	-	3,551222	-	0,7692	2965
kf_7	752,797067	y_k	4	0,000106	8,349887	0,6538	3641
kf_8	0,032870	y_r	-	71,546219	-	0,7692	2196
kf_9	2,338166	y_r	-	0,069718	-	0,7692	2619
kf_{10}	1,003871	y_r	-	0,000108	8,599668	0,7307	2374
kf_{11}	0,066392	y_{ch}	-	-	-	0,6923	2239
kf_{12}	0,242064	y_{ch}	-	-	-	0,6538	2357
kf_{13}	2,266518	y_{ch}	-	-	-	0,7307	2688
kf_{14}	2,008698	y_k	4	307,409091	0,114934	0,6923	2305
kf_{15}	25,667659	y_k	5	1,817766	7,198037	0,6538	3150
kf_{16}	1,151799	y_k	4	0,162659	6,518092	0,6538	2690
ks_1	9,116698	y_r	-	0,097286	-	0,6923	3026
ks_2	50,175752	y_r	-	0,001702	-	0,6923	3371
ks_3	278,568990	y_k	1	0,000235	9,930811	0,6538	3591
ks_4	0,012647	y_k	2	0,240849	0,026286	0,7308	2215
ks_5	7,919836	y_r	-	0,002571	-	0,6538	2639

ks_6	809,293027	y_k	5	0,000183	3,407356	0,7692	3985
ks_7	0,044067	y_{ch}	-	-	-	0,8077	2567
ks_8	599,180477	y_r	-	5,121008	-	0,6538	3318
ks_9	0,251858	y_{ch}	-	-	-	0,6154	2010
ks_{10}	5,046902	y_r	-	35,939542	-	0,6923	2294
ks_{11}	0,334784	y_{ch}	-	-	-	0,6923	2784
ks_{12}	724,359512	y_k	3	0,003628	8,409752	0,6923	3921
ks_{13}	0,091040	y_r	-	2,325025	-	0,8462	2036
ks_{14}	0,085819	y_{ch}	-	-	-	0,7308	2150
ks_{15}	0,012940	y_k	5	0,008556	2,401576	0,6154	2693
ks_{16}	214,060936	y_s	-	0,040617	0,510375	0,6154	2415

Simmetrik shifrlash algoritmi sifatida S-AES tanlab olinib, tasniflash masalasi uning shifrlash raundi kaliti bitlarini aniqlashga qaratidi. Nochiziq ma’lumotlarni tasniflash uchun mashinaviy o‘qitish va giper parametrlarni tanlash muhimdir. S-AES algoritmi tahlil qilingan bo‘lib, uning kalit bitlari va asosiy shifrlash raundlari yordamida O‘T shakllantirilgan. c_1 va c_2 shifrmatnlarining O‘T bir xil raund kalitlari orqali hosil qilingan. O‘tkazilgan tadqiqot orqali eng yuqori kalit bitini tasniflash aniqligi kf_2 – raund kalitida 88,46% ni va eng kichik tasniflash aniqligi ks_9 , ks_{15} , ks_{16} kalit bitlarida bo‘lib 61,54% ga erishildi. Raundlarga kiruvchi 48 ta bitli kalitlarni o‘rtacha tasniflash aniqligi esa 70,67% ni tashkil etdi. Bu ishda, mashinani chuqur o‘qitishga asoslangan kriptotahlil usullalarining soddalashtirilgan blokli shifrlarga qo‘llanilishi tahlil qilindi va kriptotahlil masalalariga mashinaviy o‘qitish usuliga asoslangan yondashuv taklif etildi.

Demak, ushbu tadqiqotda S-AES algoritmi misolida mashinaviy o‘qitish usullaridan foydalanib, raund kalit bitlarini tasniflash samaradorligi tahlil qilindi. Natijalarga ko‘ra, ayrim bitlarda tasniflash aniqligi 88,46% gacha yetgan bo‘lsa, o‘rtacha aniqlik darajasi 70,67% ni tashkil etdi. Bu ko‘rsatkichlar mashinani chuqur o‘qitish asosida kriptotahlil usullarining samaradorligini tasdiqlaydi. Shuningdek, nochiziq xususiyatlarga ega bo‘lgan shifrlash jarayonlarini o‘rganishda neyron tarmoqlar muhim ustunliklarga ega ekanligi aniqlandi.

Tadqiqot natijalari mashinaviy o‘qitishga asoslangan kriptotahlilning soddalashtirilgan blokli shifrlarga tatbiq etilishi mumkinligini ko‘rsatdi. Kelgusida yanada murakkab algoritmlar, xususan AES va milliy standartlarga asoslangan shifrlash tizimlariga bu yondashuvni qo‘llash istiqbolli hisoblanadi. Shuningdek, turli neyron tarmoqlar arxitekturalarini solishtirish, giperparametrlarni optimallashtirish va ma’lumotlar hajmini kengaytirish orqali kalit bitlarini aniqlash samaradorligini yanada oshirish mumkin.

FOYDALANILGAN ADABIYOTLAR:

1. Dwivedi A.D., Srivastava G. Security analysis of lightweight IoT encryption algorithms: SIMON and SIMECK // Internet of Things. 2023. T. 21. p. 100677.
2. So J. Deep Learning-Based Cryptanalysis of Lightweight Block Ciphers // Security and Communication Networks. 2020. T. 2020. p. 1–11.
3. Jain A., Kohli V., Mishra G. Deep Learning based Differential Distinguisher for Lightweight Block Ciphers.
4. Kim H. и др. Deep-Learning-Based Cryptanalysis of Lightweight Block Ciphers Revisited // Entropy. 2023. T. 25, № 7. p. 986.
5. Phan R.C.-W. Mini advanced encryption standard (mini-AES): A testbed for cryptanalysis students // Cryptologia. 2002. T. 26, № 4. p. 283–306.
6. Kuryazov D.M, Sattarov A.B, Axmedov B.B. Blokli simmetrik shifrlash algoritmlari bardoshliligini zamonaviy kriptotahlil usullari bilan baholash. O‘quv qo‘llanma. Toshkent, 2017. 224 b.
7. B.F.Abduraximov, J.R.Abdurazzoqov. Soddalashtirilgan AES (S-AES) ning kaliti haqida ma’lumotga ega bo‘lish maqsadida chuqur o‘qitishga asoslangan kriptotahlildan foydalanish // Informatika va energetika muammolari . 2023. T. 2. b. 17–26.
8. Sun B.-Y., Huang D.-S., Fang H.-T. Lidar signal denoising using least-squares support vector machine // Signal Processing Letters, IEEE. 2005. T. 12. p. 101–104.
9. Kazemi A. и др. Two-Layer SVM, Towards Deep Statistical Learning // 1st International Engineering Conference on Electrical, Energy, and Artificial

Intelligence, EICEEAI 2022. Institute of Electrical and Electronics Engineers Inc., 2022.

10. Chen P. и др. Prediction of protein B-factors using multi-class bounded SVM // Protein Pept Lett. Protein Pept Lett, 2007. Т. 14, № 2. p. 185–190.

11. Cristianini N., Shawe-Taylor J. An introduction to support vector machines and other kernel-based learning methods. 2000.

12. Burges C.J.C. A tutorial on support vector machines for pattern recognition // Data Min Knowl Discov. Kluwer Academic Publishers, 1998. Т. 2, № 2. P. 121–167.

13. Hyperopt Documentation [Электронный ресурс]. URL: https://hyperopt.github.io/hyperopt/ (дата обращения: 11.03.2024).

14. Lindauer M. и др. SMAC3: A Versatile Bayesian Optimization Package for Hyperparameter Optimization // Journal of Machine Learning Research. 2022. Т. 23, № 54. p. 1–9.

15. Shekhar S., Bansode A., Salim A. A Comparative study of Hyper-Parameter Optimization Tools // 2021 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE). IEEE, 2021. p. 1–6.

16. Parra-Ullauri J. и др. Federated Hyperparameter Optimisation with Flower and Optuna // Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing. New York, NY, USA: ACM, 2023. p. 1209–1216.