Xulosa va takliflar. Ushbu maqolada RSA va El-Gamal algoritmlariga asoslangan elektron raqamli imzo tizimlarining ishlash prinsiplari, matematik asoslari hamda imzoni hosil qilish va tekshirish bosqichlari tahlil qilindi. Tadqiqot davomida RSA algoritmida xavfsizlik katta tub sonlarni koʻpaytuvchilarga ajratish masalasining murakkabligiga, El-Gamal algoritmida esa diskret logarifmlash muammosining hisoblash jihatdan murakkab ekanligiga asoslanishi koʻrsatib berildi.

Shuningdek, algoritmlarning kalitlar bilan ishlash xususiyatlari, hisoblash jarayonlari va kriptografik barqarorligi oʻzaro solishtirildi. Tahlil natijalarida, RSA algoritmi amaliy tizimlarda koʻp qoʻllaniladi, El-Gamal algoritmi esa tasodifiy parametrlardan foydalanganligi sababli ma'lumotlarni ishonchli himoyalash imkonini beradi.

Natijada RSA va El-Gamal algoritmlariga asoslangan elektron raqamli imzo mexanizmlari zamonaviy axborot tizimlarida elektron hujjatlarning ishonchliligi, yaxlitligi va autentifikatsiyasini ta'minlashda muhim kriptografik yechimlardan biri ekanligi aniqlandi.

Foydalanilgan adabiyotlar roʻyxati:

[1]. Liu B., Blancaflor E.B. Data Security and Privacy Protection Scheme Based on EC-ElGamal in Federal Learning, 2025.

[2]. FIPS 186-5 –Digital Signature Standard (DSS). National Institute of Standards and Technology (NIST), 2023. URL: https://csrc.nist.gov/publications/detail/fips/186/5/final

[3]. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. Учебное пособие для вузов. Москва, 2005, URL: https://нэб.рф/

[4]. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С. Москва, 2002, URL: https://www.schneier.com/books/applied_cryptography/

[5]. Akbarov D.E., Xasanov P.F., Xasanov X.P., Axmedova O.P. Kriptografiyaning matematik asoslari. Toshkent, 2010.

[6]. Paar C., Pelzl J. Understanding Cryptography: A Textbook for Students and Practitioners. Springer, 2010, URL: https://link.springer.com/book/10.1007/978-3-642-04101-3

[7]. Stallings W. Cryptography and Network Security: Principles and Practice. Pearson Education, 2017, URL: https://www.pearson.com/

[8]. IEEE Std 1363-2000 – IEEE Standard Specifications for Public-Key Cryptography. IEEE, 2000. URL: https://standards.ieee.org/

[9]. ISO/IEC 18033-2:2006 – Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers. ISO/IEC, 2006. URL: https://www.iso.org/standard/37971.html

Qurbonova Mahzuna Roʻziboyevna (Mirzo Ulugʻbek nomidagi Oʻzbekiston Milliy universitetining "Axborot xavfsizligi" kafedrasi "05.01.02-Tizimli tahlil, boshqaruv va axborotlarni qayta ishlash" mutaxassisligi tayanch doktoranti (PhD); E-mail: mahzuna1214@icloud.com)

OCHIQ KALITLI KRIPTOGRAFIK ALGORITMLARNING XAVFSIZLIK MODELLARI ASOSIDA QIYOSIY BARDOSHLILIK TAHLILI

Annotatsiya. *Maqolada RSA va El-Gamal ochiq kalitli algoritmlari matematik asoslari va zamonaviy xavfsizlik modellari (IND-CPA, IND-CCA) boʻyicha qiyosiy tahlil qilingan. RSAning kichik maxfiy koʻrsatkichga asoslangan zaifligi Wiener hujumi misolida davomli kasrlar usulida isbotlangan, shuningdek, uning determinizm sababli IND-CPA xavfsiz emasligi koʻrsatilgan. El-Gamal uchun DDH farazi asosida IND-CPA xavfsizligi isbotlangan, ammo malleability xususiyati tufayli IND-CCA modellarida zaifligi aniqlangan. Natijalar resurslari cheklangan qurilmalar uchun yengil kriptografik yechimlar zarur-ligini koʻr-satadi.*

Kalit soʻzlar: *RSA; El-Gamal, ochiq kalitli kriptografiya, IND-CPA xavfsizligi, IND-CCA xavfsizligi, Wiener hujumi, DDH farazi, malleability.*

СРАВНИТЕЛЬНЫЙ АНАЛИЗ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ С ОТКРЫТЫМ КЛЮЧОМ НА ОСНОВЕ МОДЕЛЕЙ БЕЗОПАСНОСТИ

Аннотация. *В статье проведён сравнительный анализ криптографических алгоритмов с открытым ключом RSA и Эль-Гамаль на основе их математических основ и современных моделей безопасности (IND-CPA, IND-CCA). Уязвимость RSA при малом секретном показателе доказана на примере атаки Винера методом цепных дробей, а также показана недостаточность RSA для IND-CPA из-за детерминированности. Для Эль-Гамаль доказана IND-CPA-безопасность на основе предположения DDH, однако выявлена уязвимость в моделях IND-CCA из-за свойства malleability.*

Результаты указывают на необходимость лёгких криптографических решений для ресурсоограниченных устройств.

Ключевые слова: *RSA, Эль-Гамаль, криптография с открытым ключом, безопасность IND-CPA, безопасность IND-CCA, атака Винера, предположение DDH, malleability.*

COMPARATIVE ROBUSTNESS ANALYSIS OF PUBLIC-KEY CRYPTOGRAPHIC ALGORITHMS BASED ON SECURITY MODELS

Annotation. *This article presents a comparative analysis of the RSA and El-Gamal public-key algorithms based on their mathematical foundations and modern security models (IND-CPA, IND-CCA). RSA's vulnerability under a small private exponent is proven via Wiener's attack using continued fractions, and its determinism is shown to violate IND-CPA security. For El-Gamal, IND-CPA security is proven under the DDH assumption, while its malleability property is shown to break IND-CCA security. The findings highlight the need for lightweight cryptographic solutions for resource-constrained devices.*

Keywords: *RSA, El-Gamal, public-key cryptography, IND-CPA security, IND-CCA security, Wiener's attack, DDH assumption, malleablility.*

Kirish. Axborot xavfsizligi sohasida asimmetrik kriptografiya algoritmlari shifrlash, raqamli imzo va autentifikatsiyaning asosiy vositasi hisoblanadi. So'nggi yillarda IoT qurilmalari, simsiz sensor tarmoqlari va mobil platformalarning keng qo'llanilishi natijasida kriptografik algoritmlarning xavfsizlik bilan bir qatorda hisoblash samaradorligiga bo'lgan talab ham ortib bormoqda. Shu sababli klassik ochiq kalitli algoritmlarning kriptobardoshliligi va resurs sarfi o'rtasidagi muvozanatni tadqiq etish dolzarb ilmiy masala hisoblanadi.

RSA (Rivest, Shamir, Adleman, 1977) va El-Gamal (1985) algoritmlari bugungi kunda eng ko'p tadqiq etilgan va qo'llaniladigan ochiq kalitli kriptotizimlar hisoblanadi. Biroq resurslari cheklangan qurilmalarda RSA va El-Gamal algoritmlarining hisoblash murakkabligi hamda kalit boshqaruvi masalalari qo'shimcha optimallashtirishni talab etadi.

Rsa algoritmining kriptografik tadqiqi. RSA algoritmining xavfsizligi sonlarni faktorizatsiya qilish muammosiga asoslanadi. Ikkita katta tub son p va q berilganda $n = p \cdot q$ ni hisoblash oson, ammo n dan p va q ni ajratib olish hisoblash jihatidan murakkab. Kalit generatsiyasida $\varphi(n) = (p-1)(q-1)$ hisoblanib, ochiq ko'rsatkich e shunday tanlanadiki *gcd(e,* $\varphi(n)) = 1$; yopiq kalit d esa $e \cdot d \equiv 1 \ (mod \varphi(n)$ munosabatidan topiladi.

Shifrlash: $C = M^e \bmod n$. Deshifrlash: $M = C^d \bmod n$.

RSA algoritmida modulli darajaga oshirish amallari katta hisoblash xarajatlarini talab qiladi. Ayniqsa, kalit uzunligi ortishi bilan shifrlash va deshifrlash jarayonlarining bajarilish vaqti sezilarli ravishda ortadi.

RSAga nisbatan eng mashhur hujum Wiener hujumi hisoblanadi. Wiener hujumini 1990-yilda matematik Michael J. Wiener taklif qilgan. Bu hujum RSA algoritmining kichik maxfiy ko'rsatkich (small private exponent) holatidagi zaifligini ishlatadi. RSA shifrlash tizimida hisoblash tezligini oshirish maq-sadida ba'zi tizimlarda d (maxfiy kalit) ataylab kichik tanlanadi. Aynan shu holat hujumchiga samarali kriptotahlil yo'lini ochib beradi.

RSA algoritmida asosiy parametrlar quyidagicha aniqlanadi:

$$n = p \cdot q, \ e \cdot d \equiv 1 \ (mod \varphi(n))$$

Bu tenglikdan quyidagi munosabat kelib chiqadi:

$e \cdot d = k \cdot \varphi(n) + 1$ bu yerda k qandaydir butun son, shuningdek, $n = p \cdot q$ va $\varphi(n) = (p-1)(q-1)$

e ni ifodalash $e \cdot d = k \cdot \varphi(n) + 1$ har ikki tomonni d ga bo'lamiz: $e = \dfrac{k\varphi(n)+1}{d}$

endi $\Rightarrow n = p \cdot q$ bo'lgani uchun $\dfrac{e}{n} \dfrac{k\varphi(n)+1}{d \bullet p \bullet q}$

2-qadamda kasrni ikkiga ajratamiz: $\dfrac{e}{n} \dfrac{k\varphi(n)}{d \bullet p \bullet q} + \dfrac{1}{d \bullet p \bullet q}$.

Agar p va q katta tub sonlar bo'lsa, $p \bullet q \to \infty$, demak, $\dfrac{1}{d \bullet p \bullet q} \approx 0$, shuning uchun $\dfrac{e}{n} \approx \dfrac{k\varphi(n)}{d \bullet p \bullet q}$

3-qadam. Eyler funksiyasi $\varphi(n) = (p-1)(q-1)$ shuni qo'yamiz: $\frac{e}{n} \approx \frac{k}{d} \bullet \frac{(p-1)(q-1)}{p \bullet q}$

4-qadam suratni ochamiz: $(p-1)(q-1) = p \bullet q = p - q + 1$, shuning uchun

$\frac{(p-1)(q-1)}{p \bullet q} = \frac{p \bullet q - p - q + 1}{p \bullet q}$ kasrni bo'laklaymiz: $1 - \frac{1}{q} - \frac{1}{p} + \frac{1}{p \bullet q}$

5-qadam o'rniga qo'yamiz: $\frac{e}{n} \approx \frac{k}{d}(1 - \frac{1}{q} - \frac{1}{p} + \frac{1}{p \bullet q})$ endi p va q juda katta bo'lgani uchun

$\frac{1}{p} \approx 0, \frac{1}{q} \approx 0, \frac{1}{p \bullet q} \approx 0$ yakuniy natija $\frac{e}{n} \approx \frac{k}{d}$

Wiener teoremasiga ko'ra, agar quyidagi shart bajarilsa, $d < \frac{1}{3} \bullet \sqrt[4]{n}$ u holda $\frac{k}{d}$ kasr, $\frac{e}{n}$ ning davomli kasr yoyilmasida (continued fraction expansion) paydo bo'ladi va uni polinomial vaqtda hisoblash mumkin. Bu esa RSAning butun xavfsizlik asosini yo'q qiladi.

Hujum algoritmi

1-bosqich. Davomli kasr yoyilmasi

$$e = a_0 \bullet n + r_0 \rightarrow a_0 = [\frac{e}{n}]$$

$$n = a_1 \bullet r_0 + r_1 \rightarrow a_1 = [\frac{n}{r_0}]$$

$$r_0 = a_2 \bullet r_1 + r_2 \rightarrow a_2 = [\frac{r_0}{r_1}]$$

Bu jarayon chekli qadamda tugaydi (chunki qoldiqlar kamayib boradi), chunki $\frac{e}{n}$ har doim davomli kasrga yoyiladi va natijada $\frac{e}{n} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ldots}}$ hosil bo'ladi.

2-bosqich. Yaqinlashuvchilarni tekshirish davomli kasrning i yaqinlashuvchisi $\frac{k_i}{d_i}$ quyidagicha hisoblanadi: $k_{-1} = 1$, $k_0 = a_0$, $k_i = a_i \bullet k_{i-1} + k_{i-2}$; $d_{-1} = 0$, $d_0 = 1$, $d_i = a_i \bullet d_{i-1} + d_{i-2}$

Asosiy teorema Lagrange, agar $\left|\frac{e}{n} - \frac{k}{d}\right| < \frac{1}{2d^2}$ bo'lsa, u holda $\frac{k}{d}$ - bu $\frac{e}{n}$ ning yaqinlashuvchilaridan biri. Wiener shartidan $\left|\frac{e}{n} - \frac{k}{d}\right| < \frac{3k}{d\sqrt{n}} < \frac{1}{2d^2}$ ikkinchi tengsizlik $d < \frac{1}{3} \bullet \sqrt[4]{n}$ bo'lganda o'rinli. Haqiqiy $\frac{k}{d}$, albatta, yaqinlashuvchilar ichida bo'ladi.

3-bosqich. $\phi(n)$ ni hisoblash. Har bir nomzod (k_i, d_i) uchun bu hisoblanganda: Agar butun son chiqsa, $\rightarrow$ bu haqiqiy (k, d) juftligi.

Agar butun son bo'lmasa, $\rightarrow$ bu nomzod notog'ri, keyingisiga o'tish.

Agar natija butun son bo'lsa, p va q ni topish uchun quyidagi tenglamalar tizimi yechiladi:

$\phi(n) = (p-1)(q-1) = pq - p - q + 1 = n - (p+q) + 1$ ekanligidan

$$p + q = n - \varphi(n) + 1$$
$$p \cdot q = n$$

Bu ikki tenglama - p va q ni ildizlari bo'lgan kvadrat tenglama: $x^2 - (p+q)x + pq = 0$

$$p,\ q\ = \frac{\left[(p+q) \pm \sqrt{((p+q)^2 - 4n)}\right]}{2}$$

4-bosqich. Natija. RSA ning maxfiy kaliti d quyidagicha aniqlanadi: $e \cdot d \equiv 1\ (mod \varphi(n))$

$\varphi(n) = (p-1)(q-1)$ ma'lum bo'lganda, d ni kengaytirilgan Evklid algoritmi orqali toppish bu polynomial vaqtli operatsiya. Demak:

- $p, q \to \varphi(n) = (p-1)(q-1)$
- $\varphi(n), e \to d = e^{-1} \bmod \varphi(n)$

RSA ning maxfiy kaliti d to'liq oshkor bo'ldi – hujum muvaffaqiyatli.

RSA IND-CPA xavfsizligi

Yuqorida keltirilgan IND-CPA o'yin modelini (1–5-bosqichlar) RSA algoritmiga qo'llab ko'raylik. Klassik RSA shifrlash quyidagicha amalga oshiriladi: $C = M^e mod\ n$, bu yerda (e, n) – ochiq kalit. Ushbu funksiya deterministik xarakterga ega, ya'ni tasodifiy parametr ishtirok etmaydi.

Tanlov bosqichida (3-bosqich) hujumchi M_0 va M_1 ochiq matnlarni tanlaydi. Sinov bosqichida (4-bosqich) tizim $C^* = M_b^e mod n$ ni qaytaradi. Ammo 2-bosqichda hujumchiga oracle so'rovi orqali istalgan ochiq matnni shifrlash imkoniyati berilgani sababli, u oddiygina M_0 va M_1 ni o'zi shifrlab, natijalarni C^* bilan solishtirishi kifoya. Hujumchi C^* ni $M_0^e mod\ n$ va $M_1^e\ mod\ n$ qiymatlari bilan solishtiradi va ular qaysi niriga teng kelishini aniqlaydi.

Bu tenglik b bitini 100 ehtimollik bilan aniqlab beradi, ya'ni $\Pr[b' = b] = 1$, bu esa IND-CPA xavfsizlik shartini $\Pr[b' = b] \leq \frac{1}{2} + \varepsilon$ keskin buzadi. Demak, klassik RSA IND-CPA xavfsiz emas – bu xulosa jadvaldagi "bir xil xabar qayta shifrlanganda, bir xil natija hosil bo'ladi" degan kuzatishning nazariy asosidir: aynan shu determinizm hujumchiga tenglashtirish (equality test) orqali osongina g'alaba qozonish imkonini beradi.

El-Gamal esa har safar yangi tasodifiy r parametridan foydalangani uchun bir xil ochiq matn har safar boshqacha shifrmatn hosil qiladi, shu sababli yuqoridagi tenglashtirish hujumi ishlamaydi va IND-CPA xavfsizligi DDH farazi asosida isbotlanadi (yuqoridagi teoremaga qarang). Amaliyotda RSA'ning bu zaifligi OAEP (Optimal Asymmetric Encryption Padding) kabi randomizatsiyalashgan to'ldirish (padding) sxemalari yordamida bartaraf etiladi: [OBJ] ochiq matnga shifrlashdan oldin tasodifiy qiymat qo'shiladi, natijada RSA-OAEP IND-CPA (hatto IND-CCA2) xavfsizlikka erishadi. Biroq bu qo'shimcha hisoblash va formatlash xarajatini talab qiladi, bu esa resurslari cheklangan qurilmalar uchun yana bir muhim omil hisoblanadi.

EL-GAMAL ALGORITMINING KRIPTOGRAFIK TADQIQI

El-Gamal algoritmi diskret logarifm muammosiga (DLP) asoslanadi: p tub soni va uning primitiv ildizi g uchun $g^x \equiv h\ (mod\ p)$ tenglamada x ni aniqlash hisoblash murakkabligi nuqtayi nazaridan iyin masala hisoblanadi. Qabul qiluvchi x ni yopiq kalit, $h = g^x\ mod$ p ni esa ochiq kalit sifatida e'lon qiladi.

Shifrlash. Tasodifiy y tanlanib, $(c_1,\ c_2) = (g^y\ mod\ p, M \cdot h^y\ mod\ p)$

$(c_1,\ c_2) = \left(g^y\ mod\ p, M \cdot h^y\ mod\ p\right)$ yuboriladi.

Deshifrlash: $M = c_2 \cdot \left(c_1^x\right)^{-1}\ mod\ p.$

Har bir shifrlashda yangi tasodifiy y ishlatilgani sababli El-Gamal ehtimoliy shifrlash (probabilistic encryption) xususiyatiga ega bo'lib, IND-CPA xavfsizligini ta'minlaydi. Asosiy zaifliklar: o'rtadagi odam hujumi (MiTM) ochiq kalit almashuvida xavf tug'diradi; yon kanal hujumlari (timing analysis, power analysis) esa algoritmning apparat bajarilishida ma'lumot sizib chiqishiga olib kelishi mumkin. Shifrmatn hajmining ikki baravar ortishi ham amaliy qo'llanishdagi muhim cheklov hisoblanadi.

IND-CPA (Indistinguishability under Chosen Plaintext Attack) – tanlangan ochiq matn hujumi ostida farqlab bo'lmaslik xususiyatidir. Bu kriptografik xavfsizlik modeli shifrlash tizimining nazariy mustahkamligini o'lchash uchun qo'llaniladi va zamonaviy kriptografiyaning asosiy standartlaridan biri hisoblanadi.

O'yin modeli (Game-based Definition). IND-CPA xavfsizligi quyidagi o'yin orqali aniqlanadi:

• 1-bosqich – Sozlash: tizim kalit juftini yaratadi (PK, SK). Hujumchiga faqat PK beriladi.
• 2-bosqich – So‘rov bosqichi: hujumchi istalgan ochiq matnlarni shifrlata oladi (oracle so‘rovi).
• 3-bosqich – Tanlov: hujumchi ikkita teng uzunlikdagi matn tanlaydi: M_0 va M_1.
• 4-bosqich – Sinov: tizim tasodifiy $b \in \{0, 1\}$ tanlaydi va $C^* = Enc(PK, m_b)$ ni beradi.
• 5-bosqich – Taxmin: hujumchi $b' = b$ ni topishga harakat qiladi.

Xavfsizlik sharti quyidagicha ifodalanadi: $Pr[b' = b] \leq \frac{1}{2} + \varepsilon$ bu yerda ε - e’tiborsiz kichik (negligible) son. Agar bu shart bajarilsa, shifrlash tizimi IND-CPA xavfsiz deb hisoblanadi.

El-Gamal IND-CPA xavfsizligi. Ochiq kalit: (G, g, q, h), bu yerda $h = g^x$. Shifrlash quyidagi ko‘rinishda amalga oshiriladi: $C = (g^r, m \cdot h^r), r \leftarrow Z_q$

Teorema. El-Gamal algoritmi DDH (Decisional Diffie-Hellman) faraziga asosan IND-CPA xavfsizdir. DDH farazining mohiyati quyidagicha ifodalanadi:

$$(g^a, g^b, g^{ab}) \approx_c (g^a, g^b, g^c)$$

Ya’ni, hujumchi g^{ab} ni tasodifiy g^c dan hisoblash jihatidan ajrata olmaydi. Bu faraz kriptografiyada kuchli va keng tan olingan nazariy asos hisoblanadi.

Isbot sxemasi (Reduction). IND-CPA xavfsizligining isboti quyidagi kamayish (reduction) zanjiri orqali amalga oshiriladi:

IND-CPA hujumchisi A → DDH farqlovchisi B → DDH muammosi.

Agar A muvaffaqiyatli bo‘lsa, B DDHni hal qiladi. Lekin DDH hisoblash jihatidan qiyin deb faraz qilinadi, shuning uchun A ham muvaffaqiyatli bo‘la olmaydi. Bu isbot El-Gamalning IND-CPA xavfsizligini to‘liq asoslaydi.

El-Gamal IND-CCA ga qarshi xavfsiz emas. El-Gamal algoritmi IND-CPA xavfsizligiga ega bo‘lsa-da, kuchliroq modellarda zaif ekanligini ham ma’lum:

Xavfsizlik modeli	El-Gamal	Sabab
IND-CPA	Xavfsiz	DDH faraziga asoslanadi
IND-CCA1	Xavfsiz emas	Malleable shifr xususiyati
IND-CCA2	Xavfsiz emas	Multiplikativ o‘zgarish mumkin

Malleability muammosining mohiyati: agar $C = (g^r, m \cdot h^r)$ bo‘lsa, hujumchi m ni bilmasdan turib: $C' = (g^r, ? \cdot m \cdot h^r)$ ko‘rinishidagi yangi shifrni tuzishi mumkin. Bu C' matn αm ning to‘g‘ri shifri bo‘ladi. Ushbu xususiyat El-Gamalning IND-CCA modellarida xavfsiz emasligini ko‘rsatadi.

Xavfsizlik modellari taqqoslovi

Model	Ta’rif	El-Gamal
IND-CPA	Tanlangan ochiq matn	Xavfsiz
IND-CCA1	Shifrlash oldidan so‘rov	Xavfsiz emas
IND-CCA2	Shifrlash keyin ham so‘rov	Xavfsiz emas
IND-ENC	Faqat shifrlash zaif	Xavfsiz

RSA va El-Gamal algoritmlarining qiyosiy tahlili

Ko‘rsatkich	RSA	El-Gamal
Matematik asos	Katta sonlarni faktorlash muammosi	Diskret logorifmlash muammosi
Ochiq kalit	(e,n)	(p,g,y)
Maxfiy kalit	D	X
Shifrlash natijasi	Bitta shifrmatn C	(C_1, C_2) juftligi
Tasodifiy parameter	Mavjud emas	K tasodifiy soni mavjud
Bir xil xabar qayta shifrlanganda	Bir xil natija hosil bo‘ladi	Turli natijalar hosil bo‘ladi
Shifrmatn hajmi	Nisbatan kichik	Nisbatan kata
Xavfsizlik asosi	Faktorlash murakkabligi	Diskret logarifm murakkabligi

Xulosa. Ushbu tadqiqot RSA va El-Gamal assimetrik shifrlash algoritmlarining kriptografik bardoshliligini nazariy va qiyosiy jihatdan tahlil qildi. Har ikki algoritm ham zamonaviy ochiq kalitli kriptografiyaning tayanch nuqtalaridan biri bo‘lib qolmoqda, biroq ularning xavfsizlik xususiyatlari va amaliy qo‘llanilishi bir-biridan sezilarli farq qiladi.

Shunday qilib, ikkala algoritm ham resurslari cheklangan qurilmalar (IoT, simsiz sensor tarmoqlari) uchun hisoblash yukini oshiruvchi omillarga ega: RSA katta kalit uzunligini, El-Gamal esa katta shifrmatn hajmini talab qiladi. Bu holat kelgusi tadqiqotlarni ekvivalent xavfsizlik darajasini ancha qisqaroq kalitlar bilan ta’minlaydigan elliptik egri chiziqlarga asoslangan (ECC) yengil kriptografik sxemalarni ishlab chiqish tomon yo‘naltiradi.

Foydalanilgan adabiyotlar ro‘yxati:

(1). Wiener M.J. (1990). Cryptanalysis of short RSA secret exponents. IEEE Transactions on Information Theory, 36(3), p. 553–558.

(2). Boneh D., Durfee G. (1999). Cryptanalysis of RSA with private key d less than N^0.292. EUROCRYPT 1999, LNCS 1592.

(3). Goldwasser S., Micali S. (1984). Probabilistic encryption. Journal of Computer and System Sciences, 28 (2), p. 270–299.

(4). Tsiounis Y., Yung M. (1998). On the security of ElGamal based encryption. PKC 1998, LNCS 1431.

(5). Boneh D. (1998). The decision Diffie-Hellman problem. ANTS III, LNCS 1423.

(6). Hankerson D., Menezes A., Vanstone S. (2004). Guide to Elliptic Curve Cryptography. Springer.

Aralbaeva Aziza Azat qizi (Ajiniyoz nomidagi Nukus davlat Pedagogika instituti talabasi; E-mail: azizaaralbaeva00@gmail.com)

MATEMATIK MANTIQ AMALLARINING FUZZY MANTIQDAGI MATEMATIK ASOSLARI VA AMALIY QO‘LLANILISHI

Annotatsiya. *Ushbu maqolada matematik mantiq amallarining fuzzy mantiqdagi matematik asoslari hamda ularning amaliy qo‘llanilishi tahlil qilingan. Klassik va fuzzy mantiqdagi AND, OR, NOT hamda implication amallarining matematik ifodalanishi qiyosiy o‘rganilgan. Tadqiqotda matematik modellashtirish va qiyosiy tahlil usullaridan foydalanilgan. Natijada fuzzy mantiq amallarini T-norm va S-norm operatorlari asosida ifodalashning o‘ziga xos xususiyatlari yoritilib, ularning noaniq ma’lumotlarni qayta ishlashdagi afzalliklari asoslandi. Shuningdek, fuzzy mantiq amallarining sun’iy intellekt, ekspert tizimlari va avtomatik boshqaruv tizimlaridagi amaliy qo‘llanilish imkoniyatlari ko‘rsatildi.*

Kalit so‘zlar: *matematik mantiq, fuzzy mantiq, fuzzy to‘plamlar, a’zolik funksiyasi, T-norm, S-norm, mantiqiy amallar, matematik interpretatsiya, matematik modellashtirish, amaliy qo‘llanilish.*

Аралбаева Азиза Азат кызы (студентка 3 курса, Нукусский государственный педагогический институт имени Ажинияза; E-mail: azizaaralbaeva00@gmail.com)

МАТЕМАТИЧЕСКИЕ ОСНОВЫ ЛОГИЧЕСКИХ ОПЕРАЦИЙ В НЕЧЕТКОЙ ЛОГИКЕ И ОСОБЕННОСТИ ИХ ПРИМЕНЕНИЯ

Аннотация. *В данной статье рассмотрены математические основы логических операций в нечеткой логике и особенности их практического применения. Проведен сравнительный анализ математического представления логических операций AND, OR, NOT и импликации в классической и нечеткой логике. В исследовании использованы методы математического моделирования и сравнительного анализа. В результате раскрыты особенности представления логических операций в не-*