(E) ISSN: 3030-3214
Volume 4, № 3
2026

UO‘K: 004.056.55:003.26

10.70769/3030-3214.SRT.4.3.2026.13

KO‘P O‘ZGARUVCHILI KRIPTOGRAFIK TIZIMLAR VA ULARNING TAHLILI

Mustafoyev Azamat Botir o‘g‘li
“Unicon.uz” – Fan-texnik va marketing tadqiqotlari markazi MChJ, Toshkent, O‘zbekiston
Email: mustafoyevazamat01@gmail.com
ORCID ID: 0009-0002-0495-0567
Science ID: MQD-0826-0151

Annotatsiya. *Ushbu maqolada postkvant kriptografiyaning istiqbolli yo‘nalishlaridan biri hisoblangan ko‘p o‘zgaruvchili kriptografik tizimlarning nazariy asoslari, tuzilishi va xavfsizlik xususiyatlari tahlil qilingan. Ko‘p o‘zgaruvchili kvadratik tenglamalar tizimlariga asoslangan MQ (Multivariate Quadratic) va IP (Isomorphism of Polynomials) masalalarining hisoblash murakkabligi hamda ularning kriptografik tizimlar barqarorligini ta’minlashdagi o‘rni ko‘rib chiqilgan. Shuningdek, UOV (Unbalanced Oil and Vinegar) va Rainbow raqamli imzo sxemalarining tuzilishi, ishlash tamoyillari, afzalliklari va xavfsizlik jihatlari yoritilgan. Ko‘p o‘zgaruvchili kriptografik sxemalarga nisbatan qo‘llaniladigan asosiy kriptotahlil usullari va ehtimoliy hujumlar tahlil qilinib, ularning postkvant axborot xavfsizligi tizimlarida qo‘llash imkoniyatlari baholangan.*

Kalit so‘zlar: *postkvant kriptografiya, ko‘p o‘zgaruvchili kriptografiya, MQ masalasi, IP masalasi, UOV, Rainbow, raqamli imzo, kriptotahlil, axborot xavfsizligi, kvantga bardoshli kriptografiya.*

Received: 11.06.2026	Accepted: 19.08.2026	Issue publication: 28.09.2026

МНОГОПЕРЕМЕННЫЕ КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ И ИХ АНАЛИЗ

Мустафаев Азамат Ботир угли
ООО «Unicon.uz» — Центр научно-технических и маркетинговых исследований, Ташкент, Узбекистан

Аннотация. *В статье проанализированы теоретические основы, структура и особенности безопасности многовариантных криптографических систем как одного из перспективных направлений постквантовой криптографии. Рассмотрены вычислительная сложность задач MQ (Multivariate Quadratic) и IP (Isomorphism of Polynomials), основанных на системах многомерных квадратичных уравнений, а также их роль в обеспечении криптографической стойкости. Освещены структура, принципы функционирования, преимущества и аспекты безопасности схем цифровой подписи UOV (Unbalanced Oil and Vinegar) и Rainbow. Проанализированы основные методы криптоанализа и возможные атаки на многовариантные криптографические схемы, а также оценены перспективы их применения в постквантовых системах информационной безопасности.*

Ключевые слова: *постквантовая криптография, многовариантная криптография, задача MQ, задача IP, UOV, Rainbow, цифровая подпись, криптоанализ, информационная безопасность,*

квантово-устойчивая криптография.

MULTIVARIATE CRYPTOGRAPHIC SYSTEMS AND THEIR ANALYSIS

Mustafaev Azamat Botir ugli

"Unicon.uz" LLC — Center for Scientific, Technical and Marketing Research, Tashkent, Uzbekistan

Abstract. *This article analyzes the theoretical foundations, structure, and security features of multivariate cryptographic systems as one of the promising areas of post-quantum cryptography. The computational complexity of the MQ (Multivariate Quadratic) and IP (Isomorphism of Polynomials) problems based on systems of multivariate quadratic equations and their role in ensuring cryptographic security are considered. The structure, operating principles, advantages, and security aspects of the UOV (Unbalanced Oil and Vinegar) and Rainbow digital signature schemes are discussed. The main cryptanalytic methods and potential attacks against multivariate cryptographic schemes are analyzed, and the prospects for their application in post-quantum information security systems are evaluated.*

Keywords: *post-quantum cryptography, multivariate cryptography, MQ problem, IP problem, UOV, Rainbow, digital signature, cryptanalysis, information security, quantum-resistant cryptography.*

Kirish. Kvant kompyuterlarining rivojlanishi zamonaviy kriptografiya oldida jiddiy muammo tug‘dirmoqda. Piter Shor tomonidan 1994-yilda taklif qilingan kvant algoritmi RSA, ECC va Diffi-Hellman kabi keng qo‘llaniladigan algoritmlarning asosini tashkil etuvchi faktorlash va diskret logarifm masalalarini polinomial vaqtda yechish imkonini beradi. Bu esa hozirgi ochiq kalitli kriptotizimlarning kelajakda kvant kompyuterlar tomonidan buzilishi xavfini keltirib chiqarmoqda, shu sababli postkvant kriptografiya (PQC) yo‘nalishi faol rivojlanmoqda.

NIST tomonidan olib borilayotgan postkvant standartlashtirish jarayoni doirasida panjara asosidagi, kodga asoslangan, xeshga asoslangan va ko‘p o‘zgaruvchili (multivariate) kriptografiya kabi bir qator yondashuvlar taklif etilgan. Ushbu maqolada shulardan biri - ko‘p o‘zgaruvchili kriptografiya - ko‘rib chiqiladi. Uning xavfsizligi cheklangan maydon ustidagi ko‘p o‘zgaruvchili kvadratik tenglamalar sistemasini yechishning (MQ muammosi) hisoblash murakkabligiga asoslanadi va bu masala hozircha samarali kvant algoritmiga ega emas.

Ko‘p o‘zgaruvchili kriptotizimlar asosan raqamli imzo sxemalarini yaratishda qo‘llaniladi. Ular orasida Unbalanced Oil and Vinegar (UOV) va undan kelib chiqqan Rainbow sxemasi eng mashhurlaridan hisoblanadi. Rainbow NIST tanlovining final bosqichiga yetgan bo‘lsa-da, unga qarshi topilgan so‘nggi hujumlar uning xavfsizligiga shubha tug‘dirdi, bu esa sohada qo‘shimcha tadqiqotlar zarurligini ko‘rsatadi.

Mazkur maqolaning maqsadi – postkvant kriptografiyaning istiqbolli yo'nalishlaridan biri bo'lgan ko‘p o'zgaruvchili kriptografiyaning asosiy tamoyillarini, MQ va IP muammolarining hisoblash murakkabligini, shuningdek UOV va Rainbow raqamli imzo sxemalarining tuzilishi hamda ishlash prinsiplarini tahlil qilishdan iborat. Tadqiqot doirasida ushbu sxemalarning xavfsizlik xususiyatlari va amaliy qo‘llash imkoniyatlari ham ko''rib chiqiladi.

Mazkur maqolada MQ va IP muammolarining matematik mohiyati, shuningdek UOV va Rainbow sxemalarining tuzilishi, kalit generatsiyasi, imzo yaratish va tekshirish jarayonlari tahlil qilinadi.

Metodlar. *Ko‘p o‘zgaruvchili kriptografiya* (Multivariate Cryptography) - bu post-kvant kriptografiya sohasidagi istiqbolli yo‘nalishlardan biri bo‘lib, u bir nechta o‘zgaruvchilarga ega bo‘lgan polinomlar orqali kalit juftliklarini generatsiya qilish tamoyiliga asoslanadi. Ushbu yondashuvda kriptotizimlar cheklangan algebraik maydon ustida aniqlangan ko‘p o‘zgaruvchili kvadratik tenglamalar sistemasining hisoblash murakkabligidan foydalanadi. Mazkur tengla-malarni yechish algoritmik jihatdan NP-murakkab bo‘lgani sababli, bu kriptografik sxemalar klassik va kvant kompyuterlar uchun hisoblash jihatdan bardoshli deb hisoblanadi. Ko‘p o‘zgaruvchili kriptografiyada asosiy g‘oya shundan iboratki, foydalanuvchi maxfiy kalit sifatida oddiy yechiladigan polinom tizimini tanlaydi, so‘ngra uni yashirish uchun invertibel (teskari olinadigan) o‘zgarishlar bilan aralashtiradi. Ochiq kalit esa

(E) ISSN: 3030-3214
Volume 4, № 3
2026

murakkab ko‘rinishga ega bo‘lgan polinomlar tizimi bo‘ladi. Imzo yaratishda foydalanuvchi maxfiy tizimda yechim topadi, uni o‘zgartirib, ochiq tizimga moslashtiradi. Verifikatsiya esa ochiq tizimda amalga oshiriladi.

Ko‘p o‘zgaruvchili kriptografik tizimlar odatda raqamli imzo yaratish uchun ishlatiladi. Shifrlash uchun ishlatiladigan variantlar mavjud bo‘lsa-da, ular kamroq qo‘llaniladi. Eng mashhur algoritmlar orasida:

Rainbow - tez va ixcham imzo yaratish imkonini beradi, NIST tomonidan final bosqichga yetgan.

UOV (Unbalanced Oil and Vinegar) - oddiy tuzilishga ega, lekin ba’zi hujumlarga nisbatan zaifliklari bor.

GeMSS (Great Multivariate Short Signature) - juda qisqa imzolar yaratadi, lekin hisoblash jihatdan og‘irroq.

Ko‘p o‘zgaruvchili polinom funksiyalar *Ta’rif 7* (Ko‘p o‘zgaruvchili kvadratik polinom funksiya). F maydon bo‘lsin. $F: F^n \to F$ funksiyasi ko‘p o‘zgaruvchili funksiya deb ataladi. $x_1, \dots, x_n \in \mathbb{F}$ o‘zgaruvchilarga ega p polinom berilgan bo‘lsin. Agar f funksiyani $p(x_1, \dots, x_n)$ ko‘rinishida ifodalash mumkin bo‘lsa, u ko‘p o‘zgaruvchili polinom funksiya deb ataladi (agar F cheklangan bo‘lsa, bu har qanday funksiya uchun mumkin). Agar F faqatgina ikkinchi darajali yoki undan past bo‘lgan hadlarni o‘z ichiga olsa, u ko‘p o‘zgaruvchili kvadratik polinom funksiya (Multivariate quadratic (MQ) polynomial function) deb ataladi. Misol uchun, funksiya $f_1(x_1, x_2, x_3) = x_1^2 x_2 + 2x_1 x_2^2 + 3x_3 + 4$ ko‘p o‘zgaruvchili polinom funksiya (uchinchi darajali), ammo, $f_2(x_1, x_2, x_3) = x_1^2 + 2x_1 x_2 + 3x_3 + 4$ ko‘p o‘zgaruvchili kvadratik polinom funksiya hisoblanadi. $p_1, \dots, p_k$ ko‘p o‘zgaruvchili kvadratik polinom funksiyalar bo‘lsin. $\mathcal{P} = \begin{pmatrix} p_1 \\ \vdots \\ p_k \end{pmatrix}$ vektor har bir komponent uchun qo‘llanilgan funksiyalar yig‘indisi orqali $P: \mathbf{F}^n \to \mathbf{F}^k$ funksiyasi sifatida talqin qilinishi mumkin va u polinom akslantirish deb ataladi.

MQ muammosi F cheklangan maydon bo‘lsin. $p_1, \dots, p_k: F^n \to F$ ko‘p o‘zgaruvchili kvadratik polinom funksiyalar bo‘lsin. Quyidagi tenglamalar tizimi uchun $s \in \mathbf{F}^n$ yechimni topish, MQ (multivariate quadratic) muammosi deb ataladi [1]:

$$p_1(s) = 0 \ \vdots \ p_k(s) = 0$$

Ushbu muammo hisoblash jihatidan qiyin ekanligi isbotlangan.

Ko‘p o‘zgaruvchili imzo sxemalari ochiq kalitli kriptosistemalar (Multivariate public-key cryptosystems, MPKC) polinomial akslantirishlardan ochiq va shaxsiy kalitlarni ifodalash uchun foydalaniladigan konstruksiyalardir. Ammo, MPKC konstruksiyalari asosan raqamli imzo sxemalari sifatida qo‘llaniladi va shifrlash maqsadlari uchun mos emas [4].

F cheklangan maydon bo‘lsin. Berilgan xabar $m \in F$ uchun imzo $s \in F^n$ yaratishning asosiy g‘oyasi P polinomial akslantirishi ostida m obraziga (image) bir yoki bir nechta asl obrazni (pre image) hisoblashdir. Bu quyidagi keltirilgan tenglamalar tizimini echimi s ni topishga teng:

$$\begin{matrix} p_1(s) = m_1 \\ \vdots \\ p_k(s) = m_k \end{matrix} \Leftrightarrow \begin{matrix} p_1(s) - m_1 = 0 \\ \vdots \\ p_k(s) - m_k = 0 \end{matrix} \quad (1)$$

Bu yerda, $\mathcal{P} = (p_1, \dots, p_k)$ va $m = (m_1, \dots, m_k)$. $\mathcal{P}$ – akslantirish deb ataldi va ochiq kalitni taqdim etadi. MPKC sxemasini ochiq akslantirish ostida asl obrazlarni topishga imkon beradigan tarzda loyihalash mumkin, lekin MQ muammosini to‘g‘ridan-to‘g‘ri hal qilmasdan. Odatda, bu mexanizm $\mathcal{F}: F^n \to F^k$ polinomial akslantirishini o‘z ichiga oladi, u markaziy akslantirish deb ataladi. $\mathcal{F}$ akslantirishni quyidagi ikki affin akslantirishlarni qo‘llash orqali yashirish mumkin: $\mathcal{S}: F^n \to F^n$ va $\mathcal{T}: F^k \to F^k$. Hosil bo‘lgan funksiya $\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S}: F^n \to F^k$ tegishli shaxsiy kalit $(\mathcal{T}, \mathcal{F}, \mathcal{S})$ uchun ochiq kalit sifatida xizmat qiladi. Odatda, markaziy akslantirish F asl obrazlarni samarali hisoblash imkoniyatini talab qiladi. Affin akslantirishlar $\mathcal{S}$ va $\mathcal{T}$ teskarilanuvchi (invertible) bo‘lishi kerak; shuning uchun ular to‘liq rangga ega bo‘lishi talab etiladi.

MPKC (Ko‘p o‘zgaruvchilik kripto-tizmlar)ning asosiy komponenti markaziy akslantirish $\mathcal{F}$ ni loyihalashdir. Shaxsiy kalit $(\mathcal{T}, \mathcal{F}, \mathcal{S})$ haqida oldindan ma’lumotga ega bo‘lmasdan, hujumchi ochiq akslantirishni tasodifiy polinomial akslantirishdan farqlay olmaydi. Shu sababli, to‘g‘ridan-to‘g‘ri hujumning murakkabligi MQ muammosining qiyinligiga tenglashtiriladi.

Biroq, ushbu tizimning xavfsizlik farazi markaziy akslantirish $\mathcal{F}$ ga qarshi samarali hujumlar ehtimoli tufayli MQ muammosiga qaraganda kuchliroqdir. Ochiq akslantirishga to‘g‘ridan-to‘g‘ri hujum qilish o‘rniga, MPKCni buzishning muqobil usuli mavjud. G‘oya shundan iboratki, markaziy akslantirish $\mathcal{F}$ F ni $\mathcal{P}$ ga o‘zgartirish uchun zarur bo‘lgan ikkita muqobil affin akslantirishlarini topish kerak. Shunday qilib, kriptotizimga mos keluvchi ochiq akslantirish uchun boshqa shaxsy kalitlarni topish orqali hujum amalga oshirilishi mumkin. Bu mazmunda yangi muammo - polinomlar izomorfizmi (Isomorphism of Polynomials, IP) muammosini aniqlashtirish kerak [3].

IP muammosi Agar $\mathcal{P}$, $\mathcal{F}$ - $\boldsymbol{F}^n$ dan $\boldsymbol{F}^k$ ga bo‘lgan ikkita polinomial akslantirish bo‘lsa va $\mathcal{P} = (p_1, \dots, p_k)$, $\mathcal{F} = (f_1, \dots, f_k)$ deb yozilsa, shunday shartlarda agar $\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S}$ shartni qanoatlantiruvchi ikki teskarisiga ega affin akslantirishlar $\mathcal{S}: \mathrm{F}^{\mathrm{n}} \to \mathrm{F}^{\mathrm{n}}$ va $\mathcal{T}: \mathrm{F}^{\mathrm{k}} \to \mathrm{F}^{\mathrm{k}}$ mavjud bo‘lsa, $\mathcal{S}$ va $\mathcal{T}$ ni topish IP muammosi deb atalib, u yetarlicha hisoblash murakkabligiga ega hisoblanadi [2]. IP muammosini yechish MPKCni buzishi mumkin, chunki bu usul orqali maxfiy affini funksiyalarni topish mumkin. Bu esa berilgan ochiq akslantirish va tasodifiy tanlangan markaziy akslantirishga alternativ maxfiy kalitlar topilishiga olib keladi.

Rainbow imzo sxemasi ehtimoliy eng keng tarqalgan ko‘p o‘zgaruvchili imzo sxemasi bo‘lgan Unbalanced Oil and Vinegar (UOV) sxemasi bilan yaqin bog‘liq. Rainbowni tushunish uchun, avvalo, UOV ni to‘g‘ri tushunish taab etiladi.

UOV ning asosiy g‘oyasi markaziy akslantirish $\mathcal{F}$ ning o‘zgaruvchilar to‘plamini ikki o‘zaro kesishmaydigan bo‘limga ajratishdan iborat bo‘lib, bular oil (neft) va vinegar (sirka) o‘zgaruvchilar deb ataladi. Eng muhim xususiyat shundaki, $\mathcal{F}$ ning kvadratik polinomlari ikki oil o‘zgaruvchisi o‘rtasida cross-term (aralash ko‘paytuvchilar) bo‘lishiga ruxsat bermaydi. UOV umumiy holda ochiq va yopiqkalitlarni tez hisoblashni taklif qiladi hamda sodda strukturasi bilan ajralib turadi. Lekin uning kamchiligi kalitlarni nisbatan katta o‘lchamida namoyon bo‘ladi [10].

UOV sxemasi MPKC sxemasi sifatida tavsiflanadi, yuqorida tasvirlanganidek, ochiq akslantirish $\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S}: F \to F^k$ va shaxsiy polinomial akslantirishlari $(\mathcal{T}, \mathcal{F}, \mathcal{S})$ bilan. Bu sxema oil va vinegar o‘zgaruvchilarining sonini aniqlovchi o va v butun parametrlar bilan tavsiflanadi. Ushbu parametrlar markaziy akslantirish $\mathcal{F}$ tuzilishini belgilaydi, bu yerda, $k = o$ polinomial funksiyalar va $n = o + v$ o‘zgaruvchilar mavjud. Markaziy akslantirish $\mathcal{F}: F^n \to F^k$ o‘z navbatida k ta polinom funksiyalar $f_1, \dots, f_k$ dan tashkil topgan. Ular bir rangli shaklga keltiriladi, ya’ni, konstanta va chiziqli hadlar tashlab yuboriladi. U holda har bir f_r quyidagi ko‘rinishga ega bo‘ladi:

$$f_r = \sum_{i=1}^{v} \sum_{j=i}^{v} \alpha_{ij}^{(r)} x_i x_j + \sum_{i=1}^{v} \sum_{j=v+1}^{n} \beta_{ij}^{(r)} x_i x_j \quad (2)$$

Bu yerda, $x_1, \cdots, x_v$ va $x_{v+1}, \cdots, x_n$ mos holda vinegar va oil o‘zgaruvchilari. $\mathcal{F}$ markaziy akslantirish $\mathbb{F}$ dan $\alpha_{ij}^{(r)}$, $\beta_{ij}^{(r)}$ koeffitsientlariga tasodifiy qiymatlar tayinlash orqali generatsiya qilinadi [9]. Affin o‘zgartirishlar $\mathcal{S}$ va $\mathcal{T}$ ham tasodifiy koeffitsientlarni tayinlash orqali tanlanadi, agar ularning o‘zgaruvchilari teskari qiymatga ega bo‘lmasa, bu jarayon takrorlanadi. Markaziy akslantirish $\mathcal{F}$ bo‘yicha asl obrazlarni hisoblash quyidagicha amalga oshiriladi:

1-qadam: Vinegar o‘zgaruvchilarga $x_1, \dots, x_k$ (qizil bilan ajratilgan) tasodifiy qiymatlar tayinlanadi. Bu jarayon vinegar o‘zgaruvchilar o‘rtasidagi ko‘paytma natijasini doimiyga qisqartiradi, shuningdek, oil va vinegar o‘zgaruvchilarning ko‘paytmasini chiziqli hadga aylantiradi [8]:

$$f_r = \sum_{i=1}^{v} \sum_{j=i}^{v} \alpha_{ij}^{(r)} x_i x_j + \sum_{i=1}^{v} \sum_{j=v+1}^{n} \beta_{ij}^{(r)} x_i x_j \quad (3)$$

2-qadam: Buning natijasida $n - v = k$ o‘zgaruvchi, ya’ni $x_{v+1}, \cdots, x_n$ uchun k ta chiziqli tenglamalar sistemasi hosil bo‘ladi. Gaus qisqartirishini qo‘llash orqali bu sistemani yechib, qolgan oil qiymatlari $x_{v+1}, \cdots, x_n$ aniqlanadi. Agar sistema yechimga ega bo‘lmasa, vinegar o‘zgaruvchilar uchun boshqa tasodifiy qiymatlar tanlash orqali jarayon takrorlanadi.

Yuqorida aytilganidek, bu MPKC konstruktsiyasi berilgan ochiq akslantirish P bo‘yicha asl obrazlarni topishni qiyinlashtiradigan tarzda ishlab chiqilgan. Ammo, shaxsiy dekompozitsiya $\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S}$ ni bilgan holda asl obrazlarni samarali hisoblash (masalan, imzo

(E) ISSN: 3030-3214
Volume 4, № 3
2026

yaratish) mumkin bo‘ladi.

Rainbow’ning aniq na’munasi quyidagi parametrlar orqali aniqlanadi. Birinchi sath uchun vinegar o‘zgaruvchilar soni v_1. Birinchi va ikkinchi qavatlar uchun oil o‘zgaruvchilar soni o_1 va o_2. Umumiy o‘zgaruvchilar soni $n = v_1 + o_1 + o_2$ va tenglamalar soni $k = o_1 + o_2$ formula orqali aniqlanadi. Rainbowsning markaziy akslantirish $\mathcal{F}$ ning natijaviy strukturasi quyidagi ikki sathdan iborat:

1-sath: $\underbrace{x_1, \dots, x_{v_1}}_{vinegar\ o'zgaruvchilar}, \underbrace{x_{v_1+1}, \dots, x_{v_1+o_1}}_{oil\ o'zgaruvchilar}$

2-sath:

$$\underbrace{x_1, \dots, x_{v_1}, x_{v_1+1}, \dots, x_{v_1+o_1}}_{vinegar\ o'zgaruvchilar}, \underbrace{x_{v_1+o_1+1}, \dots, x_{v_1+o_1+o_2}}_{oil\ o'zgaruvchilar}$$

Bu konstruktsiya UOV holatidagi imzo o‘lchami va xabar o‘lchami o‘rtasidagi nisbati $(v+o)/o$ dan ikki sathli Rainbow holatida $(v_1 + o_1 + o_2)/(o_1 + o_2)$ ga yaxshilanadi, chunki, $v_1 < v$. Ya’ni, amalda imzolar nisbatan kichikroq bo‘ladi (bu taxminan 26% qisqarishni anglatadi) [7]. Birinchi sathda kerakli koeffitsientlar sonining qisqarishi tufayli, bu xususiyat shuningdek, xususiy kalit hajmini ham kichikroq qiladi. Biroq, so‘nggi hujumlar ushbu konstruktsiyani zaif ekanligini ko‘rsatdi, bu esa mazkur samaradorlik yutuqlarining yo‘qolishiga olib keldi (quyida keltiriladi).

Aniq kalit juftligini yaratish uchun (1-algoritm), quyidagi akslantirishlar tanlab olinadi:

- Shaxsiy markaziy $\mathcal{F}$ akslantirish $k = o_1 + o_2$ ta ko‘phad $f_1, \dots, f_k$ dan tashkil topgan bo‘lib, ularning har biri quyidagi ko‘rinishga ega:

$$f_r = \begin{cases} r \in \{1, \cdots, o_1\}\ uchun\ \sum_{i \le j \in V_1} \alpha_{ij}^{(r)} x_i x_j + \sum_{i \in V_1, j \in o_1} \beta_{ij}^{(r)} x_i x_j \\ r \in \{o_1+1, \cdots, o_1+o_2\}\ uchun\ \sum_{i \le j \in V_2} \gamma_{ij}^{(r)} x_i x_j + \sum_{i \in V_2, j \in O_2} \delta_{ij}^{(r)} x_i x_j \end{cases} \quad (4)$$

Birinchi sath, vinegar indekslari $V_1 = \{1, \cdots, v_1\}$, oil indekslari $O_1 = \{v_1 + 1, \cdots, v_1 + o_1\}$, ikkinchi qatlam, vinegar indekslari $V_2 = V_1 \cup O_1$ va oil indekslari $O_2 = \{o_1 + 1, \cdots, o_1 + o_2\}$. Koeffitsiyent $\alpha_{ij}^{(r)}, \beta_{ij}^{(r)}, \gamma_{ij}^{(r)}$ va $\delta_{ij}^{(r)}$ lar F maydondan tasodifiy tanlanadi.

- Ikki maxfiy tasodifiy tanlangan teskarisiga ega affina akslantirish: $\mathcal{T}: F \to F^k$ va $\mathcal{S}: F^n \to F^n$. Bu akslantirishlarning koeffitsiyentlari F maydondan tasodifiy tanlanadi. Agar akslantirishlar teskarisiga ega bo‘lmasa, jarayon qayta amalga oshiriladi.

Ochiq kalit: $\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S}: F^n \to F^k$.

1-algoritm Rainbow Key Generation.

Kirish: Yo‘q.

1. $\boldsymbol{\mathcal{S}} \in \boldsymbol{F^n \to F^n}$ tanlanadi.
2. $\boldsymbol{F} \in \boldsymbol{F^n \to F^k}$ tanlanadi.
3. $\boldsymbol{\mathcal{T}} \in \boldsymbol{F^k \to F^k}$ tanlanadi.
4. $\boldsymbol{\mathcal{P} = \mathcal{T} \circ F \circ \mathcal{S} \in F^n \to F^k}$ hisoblanadi.

Chiqish: ochiq kalit $\boldsymbol{\mathcal{P}}$, shaxsiy kalit $\boldsymbol{sk} = (\boldsymbol{\mathcal{T}}, \boldsymbol{F}, \boldsymbol{\mathcal{S}})$.

Yuqorida tasvirlanganidek, berilgan $m \in \{0,1\}^*$ uzunlikdagi xabar uchun haqiqiy imzo s - bu $\mathcal{P}$ ostida $H(m)$ ning asl obrazi hisoblanadi, ya’ni, $\mathcal{P}(s) = H(m)$ tenglamasi bajariladi, bunda $H: \{0,1\}^* \to F^k$ mos keluvchi kriptografik xesh funksiyasi. Akslantirishlar $\mathcal{S}$ va $\mathcal{T}$ samarali tarzda teskari hisoblanganligi sababli, ularning ostida asl obrazlarni topish oson. Markaziy akslantirish $\mathcal{F}$ ostida asl obrazlarni topish esa UOV sxemasidagi kabi amalga oshiriladi [10]:

- birinchi sath vinegar o‘zgaruvchilarini tasodifiy tanlash, ya’ni $x_1, \cdots, x_{v_1}$:

1-sath: $\underbrace{x_1, \dots, x_{v_1}}_{vinegar\ o'zgaruvchilar}, \underbrace{x_{v_1+1}, \dots, x_{v_1+o_1}}_{oil\ o'zgaruvchilar}$

- birinchi sath oil o‘zgaruvchilarining qiymatlarini topish: hosil bo‘lgan o_1 ta tenglamalarning chiziqli sistemasi yechib, birinchi sath uchun o_1 ta oil o‘zgaruvchilarining aniq qiymatlari hisoblanadi;

- birinchi sathdan olingan qiymatlarni, ya’ni, $x_1, \dots, x_{v_1+o_1}$, ikkinchi sath tenglamalariga qo‘llash.

2-sath:

$$\underbrace{x_1, \dots, x_{v_1}, x_{v_1+1}, \dots, x_{v_1+o_1}}_{vinegar\ o'zgaruvchilar}, \underbrace{x_{v_1+o_1+1}, \dots, x_{v_1+o_1+o_2}}_{oil\ o'zgaruvchilar}$$

- ikkinchi sathdagi oil o‘zgaruvchilarining qiymatlarini topish: hosil bo‘lgan o_2 ta tenglamalarning chiziqli sistemasini yechib, ikkinchi sathning qolgan oil o‘zgaruvchilarining aniq qiymatlari hisoblanadi;

- tenglama yechimi yo‘q bo‘lsa: Agar chiziqli tizimlardan biri uchun yechim topilmasa, jarayon birinchi sath vinegar o‘zgaruvchilarining boshqa tasodifiy qiymatlarini tanlashdan boshlanadi. Xabar m uchun $\mathcal{P}$ ostida haqiqiy imzoni hisoblash H funksiyasi yordamida xabarni xeshlash va keyin maxfiy akslantirishlar $\mathcal{T}$, $\mathcal{F}$ va $\mathcal{S}$ ostida asl obrazlarni topish orqali amalga oshiriladi (2-algoritm).

2-algoritm Rainbow Signature generation.

Kirish: shaxsiy kalit $\boldsymbol{sk} = (\mathcal{T}, \mathcal{F}, \mathcal{S})$, xabar $\boldsymbol{m} \in \{\mathbf{0},\mathbf{1}\}^*$.

1. $\boldsymbol{m_H} = \boldsymbol{H}(\boldsymbol{m})$ hisoblanadi.
2. $\boldsymbol{u} = \mathcal{T}^{-\mathbf{1}}(\boldsymbol{m_H})$ hisoblanadi.
3. $\mathcal{F}$ ostida $\boldsymbol{u}$ ning asl obrazi $\boldsymbol{u^{-1}}$ topiladi.
4. $\boldsymbol{s} = \mathcal{S}^{-\mathbf{1}}(\boldsymbol{u^{-1}})$ hisoblanadi.

Chiqish: imzo $\boldsymbol{s}$.

$m \in \{0,1\}^*$ xabar va $s \in \mathbb{F}^n$ imzo berilgan bo‘lsin. Agar $H(m) = \mathcal{P}(s)$ o‘rinli bo‘lsa, s imzo haqiqiy, aks holda imzo haqiqiy emas (33-algoritm).

3-algoritm Rainbow Verification.

Kirish: ochiq kalit $\mathcal{P}$, xabar $\boldsymbol{m} \in \{\mathbf{0},\mathbf{1}\}^*$, imzo $\boldsymbol{s} \in \mathbb{F}^{\boldsymbol{n}}$.

1. $\boldsymbol{m'_H} = \mathcal{P}(\boldsymbol{s})$ hisoblanadi.
2. $\boldsymbol{m_H} = \boldsymbol{H}(\boldsymbol{m})$ hisoblanadi.

Chiqish: agar $\boldsymbol{m'_H} = \boldsymbol{m_H}$ imzo haqiqiy, aks holda haqiqiy emas.

1-javal

Rainbowning uchinchi raund parametrlari

Parametrlar	$\mathbb{F}$	v_1	o_1	o_2
Level I	GF(16)	36	32	32
Level III	GF(256)	68	32	48
Level V	GF(256)	96	36	64

Natijalar. Bu konstruktsiya UOV holatidagi imzo o'lchami va xabar o'lchami o'rtasidagi $(v + o)/o$ nisbatini ikki sathli Rainbow holatida $(v_1 + o_1 + o_2)/(o_1 + o_2)$ darajasiga yaxshilaydi, chunki $v_1 < v$. Ya'ni, amalda imzolar nisbatan kichikroq bo'ladi (bu taxminan 26% qisqarishni anglatadi) [7]. Birinchi sathda kerakli koeffitsientlar sonining qisqarishi tufayli, bu xususiyat shuningdek, xususiy kalit hajmini ham kichikroq qiladi. Biroq, so'nggi hujumlar ushbu konstruktsiyani zaif ekanligini ko'rsatdi, bu esa mazkur samaradorlik yutuqlarining yo'qolishiga olib keldi.

Rainbowning uchinchi raundi uchun taklif qilingan parametrlar 2-jadvalda keltirilgan:

Keltirilgan parametrlardan ko‘rinib turibdiki, xavfsizlik darajasi oshgan sari (Level I dan Level V gacha) chekli maydon hajmi va o'zgaruvchilar soni ham ortib boradi, bu esa kalit va imzo o'lchamlarining kattalashishiga olib keladi. Shu bilan birga, ikki sathli tuzilma UOV sxemasiga nisbatan kalit va imzo hajmini optimallashtirish imkonini beradi, biroq bu samaradorlik xavfsizlikka nisbatan doimiy tekshiruvni talab qiladi, chunki markaziy akslantirishning maxsus strukturasi potensial kriptotahlil hujumlari uchun qo'shimcha imkoniyatlar yaratishi mumkin.

2-jadval

Rainbow raqamli imzo sxemasining xavfsizlik darajalari bo‘yicha asosiy parametrlari

Parametrlar	$\mathbb{F}$	v_1	o_1	o_2
Level I	GF(16)	36	32	32
Level III	GF(256)	68	32	48
Level V	GF(256)	96	36	64

Xulosa. Maqolada ko‘p o‘zgaruvchili kriptografiyaning matematik asoslari va postkvant kriptografiyadagi o‘rni tahlil qilindi. MQ va IP muammolarining hisoblash murakkabligi ko‘rib chiqilib, UOV hamda Rainbow raqamli imzo sxemalarining tuzilishi va ishlash prinsiplari o‘rganildi. Tahlil natijasida ko‘p o‘zgaruvchili kriptografiya raqamli imzo sxemalarini yaratishda istiqbolli yo‘nalishlardan biri ekanligi aniqlandi. Shu bilan birga, mavjud sxemalarning xavfsizlik va samaradorlik xususiyatlarini chuqur tadqiq etish ularni amaliyotda qo‘llash uchun muhim ahamiyatga ega.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI

[1] Albrecht, M. R., Bernstein, D. J., Chou, T., Cid, C., Gilcher, J., Lange, T., Maram, V., von Maurich, I., Misoczki, R., Niederhagen, R., Paterson, K. G., Persichetti, E., Peters, C., Schwabe, P., Sendrier, N., Szefer, J., Tjhai, C. J., Tomlinson, M., & Wang, W. (2020). Classic McEliece: Conservative code-based cryptography.

[2] Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science (pp. 124–134).

[3] Cryptology ePrint Archive, Report 2020/1343. (2020). International Association for Cryptologic Research.

[4] Patarin, J. (1996). Hidden fields equations (HFE) and isomorphisms of polynomials. In Advances in Cryptology—EUROCRYPT ’96 (pp. 33–48). Springer.

(E) ISSN: 3030-3214
Volume 4, № 3
2026

[5] Kipnis, A., & Shamir, A. (1998). Cryptanalysis of the Oil and Vinegar signature scheme. In Advances in Cryptology—CRYPTO ’98 (pp. 257–266). Springer.
[6] Ding, J., & Schmidt, D. (2005). Rainbow, a new multivariable polynomial signature scheme. In Applied Cryptography and Network Security—ACNS 2005 (pp. 164–175). Springer.
[7] Kipnis, A., Patarin, J., & Gaborit, P. (1999). Unbalanced Oil and Vinegar signature schemes. In Advances in Cryptology—EUROCRYPT ’99 (pp. 206–222). Springer.
[8] Ding, J., Yang, B.-Y., Chen, C.-H. O., Chen, M.-S., & Cheng, Y. Rainbow signature: A new multivariable polynomial signature scheme. Cryptology ePrint Archive.
[9] Bernstein, D. J., Buchmann, J., & Dahmen, E. (Eds.). (2009). Post-quantum cryptography. Springer.
[10] Cartor, R., Cartor, M., Lewis, M., & Smith-Tone, D. (2022). IPRainbow. In Post-Quantum Cryptography: 13th International Conference, PQCrypto 2022. Springer. https://doi.org/10.1007/978-3-031-17234-2_9

Maqolaga iqtibos keltirish | Как цитировать статью | How to cite this article

Mustafoyev, A. B. (2026). Ko‘p o‘zgaruvchili kriptografik tizimlar va ularning tahlili. Sanoatda raqamli texnologiyalar, 4(3). https://doi.org/10.70769/3030-3214.SRT.4.3.2026.13