International Journal of Applied Mathematics
Volume 38 No. 7s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

TRIAD ANALYSIS BY DESIGN, SECURITY, AND EVOLUTION OF HFE, MI,AND OIL-VINEGAR CRYPTOSYSTEMS

Rishika Vishwakarma[1], Namita Tiwari[2]
[1]Department of Mathematics, School of Basic Sciences, Chhatrapati Shahu Ji Maharaj University, Kanpur. Email: vis.rishi127@gmail.com

[2]Department of Mathematics and Computer Application, Chhatrapati Shahu Ji Maharaj University, Kanpur. Email: namitatiwari@csjmu.ac.in

Corresponding author:- Namita Tiwari

Abstract:

A well-known contender in the field of post-quantum cryptography is Multivariate Public Key Cryptography (MPKC), which provides security based on the computational difficulty of solving systems of multivariate quadratic equations over finite fields. The foundational trinity of the suggested schemes the Hidden Field Equations (HFE), Matsumoto-Imai (MI), and Oil-Vinegar (OV) cryptosystems has greatly influenced the development of MPKC. These three cryptosystems are reviewed in this work in a unified and comparative manner, with an analysis of their algebraic structures, key generation mechanisms, encryption and signature procedures, and known cryptanalytic attacks. The study clarifies each scheme's advantages, disadvantages, and changes over time by following its historical evolution and emphasizing its fundamental design ideas. Their contribution to standardization initiatives and their ability to withstand new quantum threats are highlighted in particular. In order to facilitate future research and optimization in safe, effective, and scalable multivariate cryptosystems for the post-quantum era, the paper attempts to offer a comprehensive knowledge.

Keyword: Hidden Field Equation, Matsumoto-Imai, Oil-Vinegar, Multivariate Cryptosystem, Post-Quantum Cryptography,

1. Introduction

Quantum computers—devices that use quantum mechanical processes to solve mathematical problems that are challenging or unsolvable for traditional computers—have been the subject of extensive research in recent years. Many of the public-key cryptosystems in use today could be cracked by large-scale quantum computers if they are ever constructed. The integrity and confidentiality of digital communications on the Internet and elsewhere would be gravely jeopardized by this. Post-quantum cryptography, often known as quantum-resistant cryptography, aims to create cryptographic systems that are safe from both classical and quantum computers while still being able to interact with current networks and communications protocols. Multivariate public-key cryptosystems have been examined by the National Institute of Standards and Technology (NIST) as possible contenders for post-quantum cryptography standards.

Received: August 08 ,2025

International Journal of Applied Mathematics
Volume 38 No. 7s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

One of the primary families of post-quantum cryptosystems is multivariate public-key cryptography, or MPKC for short. It is becoming more and more recognized as a potential substitute for traditional public-key schemes like RSA and DSA. A collection of randomly selected nonlinear multivariate polynomial equations over a finite field is NP-hard to solve, according to a complexity theory result. Although it is generally accepted that quantum computers are unlikely to provide an edge in this type of problem, it has not yet been shown that they can solve a set of multivariate polynomial equations efficiently. For nearly a decade, the world's leading cryptographers have been collaborating with the National Institute of Standards and Technology (NIST) to create new algorithms that will guard against the looming threat of quantum computers. In August 2024, NIST also released the much awaited FIPS 203, 204, and 205 encryption standards.

For the cyber security industry and the billions of people who rely on digital trust to safeguard their data and guarantee secure online conversations, what does this mean? Let's take a closer look at the standards and the implementation plan. As the technology is still in its infancy, quantum computers are rather small today. But because they're evolving so swiftly, cyber security experts are becoming concerned. We predict the deployment of cryptographically relevant quantum computers (CRQCs) within the next 5 to 10 years. For good reason, this rapidly evolving technology is causing alarm. CRQCs will put data security and network security standards at risk by interfering with the asymmetric encryption methods that are already employed globally to protect anything from private communications to online banking. Although five to ten years may seem like ample time to guard against a threat in the future, attackers are already using the data breach technique known as *"harvest now, decrypt later,"* which involves gathering encrypted data now and keeping it until decryption is available due to quantum computing.

The solution lies in new quantum-resistant encryption techniques based on difficult mathematical problems that even quantum computers cannot solve. NIST has done just that with FIPS 203, 204, and 205, standards that provide detailed instructions on how to use the new algorithms to protect internet traffic, ensuring robust defence against the quantum attacks we know are coming. Although the methods described in FIPS 203, 204, and 205 contain many technical details, their mathematical complexity makes them inherently resistant to quantum computing attacks. By using these methods, systems can maintain a high level of security even in a future where quantum computing dominates.

Quantum-resistant algorithms are designed to provide strong encryption that can withstand attacks from even the most powerful quantum computers, protecting the encryption and decryption operations from unauthorized parties. These algorithms can be categorized into several classes, each with unique benefits and drawbacks.

Lattice Based Cryptography: The complexity of resolving issues pertaining to lattices (geometric structures) is the foundation of lattice-based cryptography. renowned for its effectiveness and robust security guarantees.

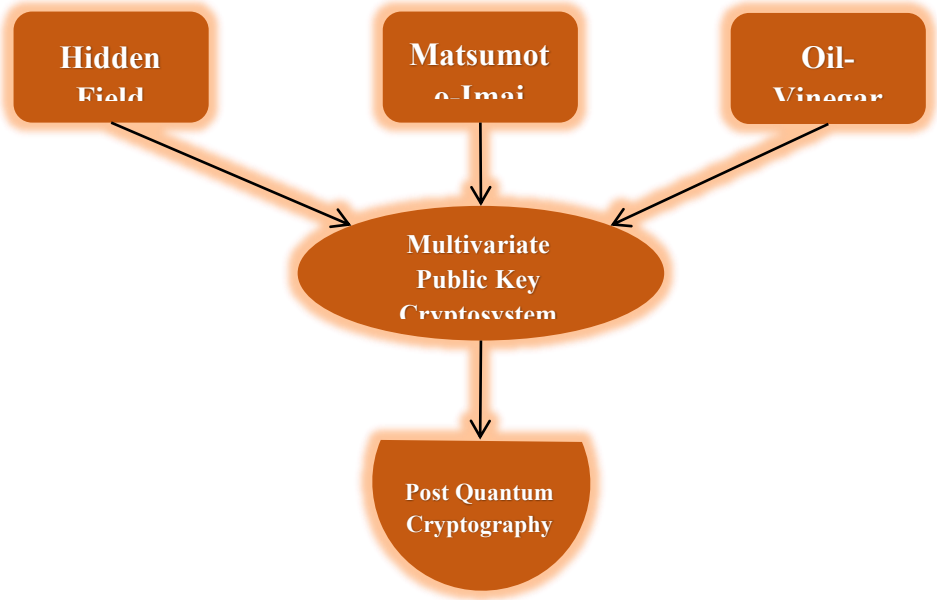
Code Based Cryptography: The difficulty of deciphering random linear codes is the foundation of code-based cryptography. renowned for simplicity and speed.

Received: August 08 ,2025

International Journal of Applied Mathematics
Volume 38 No. 7s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Hash Based Cryptography: Use cryptographic hash functions, which are one-way functions that are challenging to reverse, in hash-based cryptography. Their extensive background in security analysis is much appreciated.

Multivariate Cryptography: The difficulty of solving systems of multivariate polynomial equations over finite fields is the foundation of multivariate cryptography. Provide benefits in essential size and prospective performance.



igure 1.1 Post Quantum Cryptography

2. Timeline of Multivariate Public Key Cryptosystems HFE

In 1996, Jacques Patarin [5] proposed two asymmetric algorithms—HFE and IP—as improvements to the Matsumoto-Imai scheme, using multivariate polynomials over finite fields. These systems are resistant to known attacks and rely on the NP-complete problem of solving such equations. Although the basic HFE was attacked by Shamir and Kipnis [6] in 1999. A more secure version called QUARTZ [7] was introduced in 2001 by Patarin, Courtois, and Goubin. QUARTZ offers 128-bit digital signatures, strong resistance to attacks, and "double-layered" (combinatorial and algebraic) security. Its public key is 71 KB, and no efficient attack exists against it for chosen parameters. Between 2004 and 2009, significant developments occurred in multivariate cryptography. In 2004, Wolf and Preneel [16] analyzed HFE and its variants (HFE- and HFEv), proposed secure versions of the Quartz signature scheme, and addressed known attacks. In 2005, Wolf [18] further explored MQ systems and showed their application in product keys and electronic stamps, though they remain vulnerable to Patarin's related-message attacks [19]. In 2008, Chia-Hsin et al. [20] introduced THFE, a multivariate HFE variant over odd characteristic fields, offering better performance and resistance to known attacks. In 2009, Billet and Macario-Rat [21] fully broke the Square encryption and Square-Vinegar signature systems, requiring about 2^{35} operations. Between 2013 and 2024, several advancements were made in HFE based multivariate cryptography. In 2013, Bettale et al. [31] proposed improved key recovery

Received: August 08 ,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

attacks on HFE in both odd and characteristic-2 fields, showing HFE to be more secure than Multi-HFE. In 2014 Ding et al. [37] introduced ZHFE, using two high-rank HFE polynomials and Hamming weight three polynomials to enhance security and efficiency. In 2015, Petzoldt et al. [32] proposed Gui, an HFEv based signature algorithm that is ~100x faster than QUARTZ, with performance comparable to RSA and ECDSA. Also, Zhang et al. [38] introduced MI-T-HFE, which includes a special trapdoor and offers better efficiency and smaller public keys than QUARTZ, but with longer signatures. In 2017, Petzoldt et al. [33] presented HMFEv, a variant of Multi HFE using vinegar variation, which is efficient in memory and secure against rank attacks. In 2018, Ikematsu et al. [36] introduced HFE Rainbow Plus (HFERP), a secure encryption scheme that replaces SRP's Square polynomial with HFE to resist MinRank attacks while keeping low ciphertext expansion. In 2020, Patarin et al. [34] analyzed attacks on MPKC signatures, provided security parameters (80 to 256 bits), and highlighted the impact of hash-oracle access cost on attack feasibility. In 2024, Patarin et al. [35] proposed HFE-IP, a new signature system using Feistel-Patarin techniques to achieve ultra-short signatures and compact public keys.

MI

The Matsumoto-Imai public key scheme (1983) [1] was designed for fast signatures using $GF(2^m)$ substitution polynomials. However, it was found vulnerable due to shift and inverse operations, as shown by Delsarte et al. (1985) [2]. To build faster asymmetric cryptosystems, Matsumoto and Imai (1985) [3] proposed alternative algebraic methods using Univariate polynomials over finite commutative rings and multivariate polynomial tuples over finite fields, offering faster encryption than RSA. In 1988, Matsumoto and Imai [4] proposed the asymmetric cryptosystem C*, suitable for both encryption and digital signatures. It is considered secure because inverting its public key, defined by an n-tuple of n-variate polynomials, is extremely difficult. In 1995, Jacques Patarin [8] showed that the original Matsumoto-Imai [4] (MI) system was insecure due to its exploitable field structure. In 1996, he proposed a 64-bit asymmetric signature scheme [9] that remains unbroken but is inefficient and lacks formal security proof. Later, in 1998, Patarin, Courtois, and Goubin [10] introduced C^{+-}, a variant of the C scheme designed to resist known attacks, including Patarin's own [3]. From 2001 to 2009, several enhancements to the Matsumoto-Imai (MI) system were proposed. In 2001, Patarin, Courtois, and Goubin [22] introduced the FLASH algorithm and its faster variant SFLASH, featuring smaller public keys. In 2003, [23] they released SFLASHv3 with expanded parameters. In 2004, Jintai Ding [24] proposed the Perturbed MI (PMI) scheme, and in 2005, introduced PMI+ [25], which uses external perturbation to resist differential attacks. In 2009, Rosenthal et al. [26] developed MI-TTM by combining MI with the Tame Transformation Method, offering improved resistance to various attacks. From 2015 to 2021, several PFLASH-based and modifier-driven advancements in multivariate cryptography were introduced. In 2015, Chen et al. [39] proposed PFLASH, a digital signature scheme for smart cards, derived from SFLASH (broken in 2007) with similar performance.Also, Zhang et al. [38] introduced the MI-T-HFE cryptosystem, combining MI, triangular perturbation, and HFE polynomials. In 2017, Cartor and Smith-Tone [41]

Received: August 08 ,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

developed EFLASH, an encryption-oriented extension of PFLASH based on C* schemes. In 2021, Daniel Smith-Tone [40] introduced QC* using a nonlinear modifier Q inspired by relinearization. Q transforms any quadratic map into a UOV-type map, enabling efficient inversion. By applying Q to the Step-wise Triangular System (STS), he created QSTS, humorously turning weak encryption schemes into secure signature systems.

OV

In 1997, Patarin [11] introduced the Oil-Vinegar (OV) cryptosystem, a multivariate public key cryptosystem (MPKC) based on the difficulty of solving quadratic equations over finite fields. It uses two types of variables oil and vinegar for key construction. Although the original OV scheme was broken by Kipnis and Shamir [12], Patarin and others [13] proposed Unbalanced Oil and Vinegar (UOV) in 1999, which uses more vinegar than oil variables. In 2005, Ding et al. [14] introduced the Rainbow signature scheme, a multi-layered extension of UOV aimed at improving efficiency. That same year, Wolf et al. [15] highlighted significant security concerns in UOV that need to be addressed in signature scheme design. In 2005, Ding et al. [27] introduced the Rainbow signature scheme, a multi-layered extension of the UOV scheme designed for greater efficiency. That same year, Wolf et al. [28] identified critical security flaws in UOV that must be addressed in signature scheme design. In 2010, Petzoldt et al. [29] proposed the Cyclic Rainbow scheme, which significantly reduces the public key size of Rainbow by applying cyclic structures. In 2011, Sakumoto et al. [42] proved UOV and HFE could achieve EUF-CMA in the random oracle model with modifications. In 2012–2014, Yasuda, Thomae, Petzoldt, and Ding introduced optimized Rainbow variants like NC-Rainbow [43], Matrix-based Rainbow [45], NT-Rainbow [46], and combined versions, aiming to reduce key sizes (up to 76%) and improve signature speed (up to 55%). Thomae [44], however, challenged NC-Rainbow's security. In 2013–2017, Innovations included LRS-based UOV (Petzoldt) [47], Circulant Rainbow (Peng) [50], and LUOV (Beullens) [52], all focusing on reducing key sizes and enhancing efficiency. Circulant Rainbow was three times faster than classic Rainbow.In 2019–2021, New attacks were proposed on LUOV (Ding, Koksal) [53], exploiting its lifted structure. In 2021, Variants like QR-UOV proposed by Hiroki et. al. [56] emerged, leveraging quotient ring representations to reduce public key size without compromising signature size. In 2022–2023, Rainbow faced key recovery attacks (Beullens) [58], prompting new schemes like TriRainbow [59], TUOV [60], VDOO [62], and fault-based attacks on UOV [61]. These aimed at stronger security (against Beullens attack), better Gaussian elimination efficiency, and reduced signature time. In 2024, Kundu et al. [63] integrated secure masking into UOV to mitigate side-channel attacks (SCA). In 2025, Gupta et al. [64] proposed SCUOV (Salted Cubic Unbalanced Oil and Vinegar), the latest OV family variant.

Received: August 08 ,2025

International Journal of Applied Mathematics
Volume 38 No. 7s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Table 2.1 Timeline of Multivariate Public Key Cryptosystems

Year	HFE	MI	OV
1981-1990	---	1983 Matsumoto-Imai [1] 1985 Matsumoto and Imai [3] 1988 Matsumoto and Imai [4]	---
1991-2000	1996, Jacques Patarin [5] 1999, Shamir and Kipnis [6]	1995 Jacques Patarin [8] 1996 Jacques Patarin [9] 1998 Patarin, Courtois, and Goubin [10]	1997 Patarin [11] 1999 Patarin et. al. [13]
2001-2010	2001, Patarin, Courtois, and Goubin [7] 2004, Wolf and Preneel [16] 2005, Wolf [18] 2008, Chia-Hsin et al. [20] 2009, Billet and Macario-Rat [21]	2001 Patarin, Courtois, and Goubin [22] 2003 Patarin, Courtois, and Goubin [23] 2004 Jintai Ding [24] 2005 Jintai Ding [25] 2009 Rosenthal et al. [26]	2005 Ding et al. [14] 2005 Wolf et al. [28] 2005, Ding et al. [27] 2005 Wolf et al. [28] 2010 Petzoldt et al. [29]
2011-2025	2013, Bettale et al. [31] 2014 Ding et al. [37] 2015 Petzoldt et al. [32] 2015 Zhang et al. [38] 2017 Petzoldt et al. [33] 2018 Ikematsu et al. [36] 2020 Patarin et al. [34] 2024 Patarin et al. [35]	2015 Chen et al. [39] 2015 Zhang et al. [38] 2017 Cartor and Smith-Tone [41] 2021 Daniel Smith-Tone [40]	2011, Sakumoto et al. [42] 2012 Yasuda et. al. [43] 2012 Thomae [44] 2013 Yasuda et. al. [45] 2014 Yasuda et. al. [46] 2013 Petzoldt et. al. [47] 2017 Peng et. al.[50] 2017 Beullens et. al. [52] 2019 Ding et. al. [53] 2021 Hiroki et. al. [56]

Received: August 08 ,2025

International Journal of Applied Mathematics
Volume 38 No. 7s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

			2022 Beullens [58] 2023 Gangulay et. al.[59] 2023 Ding et. al. [60] 2022 Hiroki et. al. [61] 2024 Gangulay et. al. [62] 2024 Suparna et. al.[63] 2025 Gupta et. al. [64]

3. Mathematical Algorithm: HFE, MI and OV

Steps	MI Scheme	HFE Scheme	OV Scheme
Notations	$\mathbb{k}$: a finite field of cardinality p $p(X) \in \mathbf{k}[X]$: an degree n irreducible polynomial over $\mathbb{k}$ $\mathcal{K} = \mathbf{k}[X]/\mathbf{p}(X)$: a extension field of $\mathbb{k}$ having degree n $\psi: \mathbb{k}^n \rightarrow K$: The standard isomorphism given by: $\psi(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i X^{i-1}$ $\mathcal{F}: \mathbf{K} \rightarrow \mathbf{K}$: the central bijective map given by: $\mathcal{F}(Y) = Y^{p^\theta+1}$ where $Y \in$ K, $0 < \theta <$ n and $\gcd(p^n - 1, p^\theta + 1) = 1$ $\dot{\mathcal{F}}: \mathbb{k}^n \rightarrow \mathbb{k}^n$: a map given by: $\dot{\mathcal{F}} = \psi^{-1} \circ \mathcal{F} \circ \psi$	$\mathbb{k}$: a finite field of cardinality p $\mathcal{K}$: a degree n extension field of $\mathbb{k}$ $\psi: \mathbb{k}^n \rightarrow K$: The standard isomorphism $\mathcal{F}: \mathbf{K} \rightarrow \mathbf{K}$: the central bijective map: $\mathcal{F}(X) = \sum_{i,j=0}^{p^i+p^j \le \mathcal{D}} a_{ij} X^{p^i+p^j} + \sum_{i=0}^{q^i \le \mathcal{D}} b_i X^{p^i} + c$ where $a_{ij}, b_i, c \in$ K $\dot{\mathcal{F}}: \mathbb{k}^n \rightarrow \mathbb{k}^n$: a quadratic map given by: $\dot{\mathcal{F}} = \psi^{-1} \circ \mathcal{F} \circ \psi$ $\mathcal{T}_1, \mathcal{T}_2: \mathbb{k}^n \rightarrow \mathbb{k}^n$: two invertible map.	$\mathbb{k}$: a finite field having p elements $o, \mathbf{v}$: Integers o : taken number of equations $n = \mathbf{o} + \mathbf{v}$: taken number of variables $\mathcal{V} = \{1, \ldots, v\}$ and $\mathbf{O} = \{v + 1, \ldots, n\}$: Index sets $u_i (i \in \mathcal{V})$: Vinegar Variables $u_i (i \in \mathcal{O})$: Oil Variables $\mathcal{H}: \{0,1\}^* \rightarrow \mathbb{k}^o$: Hash Function $\mathcal{T}: \mathbb{k}^n \rightarrow \mathbb{k}^n$: an affine map. $\mathcal{F} = (f^{(1)}, \ldots, f^{(o)}): \mathbb{k}^n \rightarrow \mathbb{k}^o$: an OV central map having $f^{(1)}, \ldots, f^{(o)}$

Received: August 08 ,2025

International Journal of Applied Mathematics

Volume 38 No. 7s 2025,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

	$\boldsymbol{\mathcal{T}_1, \mathcal{T}_2}: \boldsymbol{\mathcal{k}^n} \longrightarrow \boldsymbol{\mathcal{k}^n}$: two invertible map. $\boldsymbol{\mathcal{P} = \mathcal{T}_1 \circ \dot{\mathcal{F}} \circ \mathcal{T}_2}$: a composed map An integer $\boldsymbol{\mathcal{h}}$ with $\mathcal{h}(\mathcal{p}^{\theta} + 1) = 1 \bmod (\mathcal{p}^n - 1)$ for inverting the central map $\mathcal{F}$: $\mathcal{F}^{-1}(\mathcal{X}) = \mathcal{X}^{\mathcal{h}} = \mathcal{Y}^{\mathcal{h}(\mathcal{p}^{\theta}+1)} = \mathcal{Y}^{\mathcal{h}(\mathcal{p}^n-1)+1} = Y$ $\mathcal{H}: \{0,1\}^* \longrightarrow \mathcal{k}^n$: Hash Function	$\boldsymbol{\mathcal{P} = \mathcal{T}_1 \circ \dot{\mathcal{F}} \circ \mathcal{T}_2}$: a composed map	polynomials of the form: $\mathcal{f}^{(i)} = \sum_{\mathcal{j},\mathcal{k} \in \boldsymbol{\mathcal{V}}} a_{\mathcal{j},\mathcal{k}}^{(i)} \mathcal{u}_{\mathcal{j}} \mathcal{u}_{\mathcal{k}} + \sum_{\mathcal{j} \in \boldsymbol{\mathcal{V}}, \mathcal{k} \in \boldsymbol{\mathcal{O}}} \mathcal{b}_{\mathcal{j}.\mathcal{k}}^{(i)} \mathcal{u}_{\mathcal{j}} \mathcal{u}_{\mathcal{k}} + \sum_{\mathcal{j} \in \boldsymbol{\mathcal{V}} \cup \boldsymbol{\mathcal{O}}} c_{\mathcal{j}}^{(i)} \mathcal{u}_{\mathcal{j}} + \mathcal{d}^{(i)},$ $where\ i = 1, \ldots, \mathcal{o}$
Key Generation	**Public Key:** the composed map $\boldsymbol{\mathcal{P}}$ **.** **Private Key:** two invertible linear maps $\boldsymbol{\mathcal{T}_1, \mathcal{T}_2}$ and integer $\boldsymbol{\mathcal{h}}$	**Public Key:** the multivariate quadratic map $\mathcal{P}: \mathcal{k}^n \longrightarrow \mathcal{k}^n$ **Private Key:** $\mathcal{T}_1, \mathcal{F}\ and\ \mathcal{T}_2$	**Private Key:** $\mathcal{F} = \mathcal{k}^n \longrightarrow \mathcal{k}^{\mathcal{o}}$ and $\mathcal{T}: \mathcal{k}^n \longrightarrow \mathcal{k}^n$ **Public Key:** a composed map $\mathcal{P} = \mathcal{F} \circ \mathrm{T}$
Encryption	Plaintext: $\mathcal{u} \in \mathcal{k}^n$ Compute $\mathcal{v} = \mathrm{P}(\mathcal{u}) \in \mathcal{k}^n$	Plaintext: $\mathcal{u} \in \mathcal{k}^n$ Evaluate $\mathcal{v} = \mathrm{P}(\mathcal{u}) \in \mathcal{k}^n$	---
Decryption	Ciphertext: $\mathcal{v} \in \mathcal{k}^n$ Compute : $x = \mathcal{T}_1^{-1}(\mathcal{v}) \in \mathcal{k}^n$ $\mathcal{X} = \psi(\mathrm{x}) \in \mathrm{K}$ $\mathcal{Y} = \mathcal{F}^{-1}(\mathcal{X}) \in \mathrm{K}$ $\mathcal{y} = \psi^{-1}(\mathcal{Y}) \in \mathcal{k}^n$ $\mathcal{u} = \mathcal{T}_2^{-1}(\mathcal{y}) \in \mathcal{k}^n$ Here $\mathcal{u}$ is the required plaintext.	Ciphertext: $\mathcal{v} \in \mathcal{k}^n$ Compute : $x = \mathcal{T}_1^{-1}(\mathcal{v}) \in \mathcal{k}^n$ $\mathcal{X} = \psi(\mathrm{x}) \in \mathrm{K}$ Evaluate all the solutions of $\mathcal{F}(\mathcal{Y}) = \mathrm{X}$ i.e. $\mathcal{Y}_1, \ldots, \mathcal{Y}_{\mathcal{k}}$ Now, for each $\mathcal{Y}_i (where\ i = 1, \ldots, \mathcal{k})$, compute $\mathcal{y}_i = \psi^{-1}(\mathcal{Y}_i)$ At last, compute the plaintext $\mathcal{u}_i = \mathcal{T}_2^{-1}(\mathcal{y}_i)$ There is at least one solution that matches the right plaintext for every	---

Received: August 08 ,2025

International Journal of Applied Mathematics
Volume 38 No. 7s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

		ciphertext. There are a number of methods to differentiate between legitimate and fraudulent plaintext candidates, such as hash functions or repetition inside the plaintext).	
Signature Generation	Document: d Calculate the hash value $v = \mathcal{H}(d) \in k^n$ $x = T_1^{-1}(v) \in k^n$ $X = \psi(\mathrm{x}) \in \mathrm{K}$ $Y = F^{-1}(X) \in \mathrm{K}$ $y = \psi^{-1}(Y) \in k^n$ $u = T_2^{-1}(y) \in k^n$ Here u is the required signature.	Document: d Starting from $r = 0$, compute $v = \mathcal{H}(d \parallel r)$ and follow steps: $x = T_1^{-1}(v) \in k^n$ Find all the solutions $Y_1, \ldots, Y_k$ of $\mathcal{F}(Y) = \mathrm{X}$ If there is no solution to the equation, increase the counter r, calculate the new hash value $v = \mathcal{H}(d \parallel r)$, and repeat the previous step. By the result Y, we compute: $y = \psi^{-1}(Y)$ At lat, the HFE signature is computed as: $u = T_2^{-1}(y \in k^n)$ Send (u, r) to the verifier.	Document: d Calculate the hash value $v = \mathcal{H}(d) \in k^o$ Find a pre-image $y \in k^n$ of v under the central map $\mathcal{F}$. Subtitute chosen random value of vinegar variables $y_1, \ldots, y_v$ into $f^{(1)}, \ldots, f^{(o)}$. Use Gaussian elimination to solve the resulting linear system of o equations in the o Oil variables $y_{v+1}, \ldots, y_n$. Select other values for the vinegar variables, then try again if the system is unable to produce a solution. Compute signature $u = T^{-1}(y) \in k^n$ Here u is the required signature.
Signature Verification	To verify, one compute: $v = \mathcal{H}(d) \in k^n$ $v' = \mathrm{P}(u) \in k^n$ If $v = \mathrm{v}'$, then the signature is valid otherwise invalid.	To check the authenticity of a signature (u, r), one compute: $v = \mathcal{H}(d \parallel r) \in k^n$ $v' = \mathrm{P}(u) \in k^n$	To verify, one compute: $v = \mathcal{H}(d) \in k^o$ $v' = \mathrm{P}(u) \in k^o$ If $v = v'$, then the signature is valid

Received: August 08 ,2025

International Journal of Applied Mathematics
Volume 38 No. 7s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

		If $\mathcal{v} = \mathrm{v}'$, then the signature is valid otherwise invalid.	otherwise invalid.

4. A Comparative analysis of MPKCs

Feature	**HFE (Hidden Field Equations)**	**MI (Matsumoto-Imai)**	**OV (Oil-Vinegar)**
Inventor / Year	Patarin, 1996 [19]	Matsumoto & Imai, 1988 [4]	Patarin, 1997 [11]
Underlying Field	Extension field $\mathcal{F}_{q^n}$	Extension field $\mathcal{F}_{q^n}$	Finite field $\mathcal{F}_{q^n}$ (typically q=2)
Structure	Hidden polynomial over extension field	Monomial map over extension field	Quadratic polynomials with oil/vinegar variables
Public Key Size	~ 20–100 KB (depends on parameters)	~ 20–100 KB	~ 10–100 KB (variant dependent)
Private Key Size	Small (compact representation)	Small	Small to medium
Efficiency (Signature/Decryption)	Moderate	Moderate	High
Efficiency (Encryption/Verification)	Fast	Fast	Fast
Quantum Resistance	Yes (believed)	Yes (believed)	Yes (believed)

Received: August 08 ,2025

International Journal of Applied Mathematics
Volume 38 No. 7s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Feature	HFE (Hidden Field Equations)	MI (Matsumoto-Imai)	OV (Oil-Vinegar)
Security Basis	Hardness of solving HFE systems	Hardness of structured polynomial inversion	MQ problem + variable separation
Main Attacks	- Gröbner basis attack - Kipnis-Shamir (for HFE-)	- Differential attacks - Linearization	- Kipnis-Shamir (for balanced OV) - UOV is more secure
Recommended Variant	HFEv-, HFEv- with vinegar variables	MI+ (modified variant)	UOV (Unbalanced Oil-Vinegar)
Standardization Status	NIST Round 1 candidate (HFEv-)	Broken in original form	NIST Round 3 (e.g., Rainbow/UOV)

5. Possible Attacks on MPK Cryptosystems

Cryptosystem	Attack Name / Type	Description	Reference
HFE	Algebraic Attacks	Exploiting the sparsity of the HFE polynomials to recover private key	Patarin (1995) [19]
HFE	Gröbner Basis Attack	Solving the MQ system using Gröbner basis computation	Faugère et al. (2003) [65]
	Kipnis-Shamir Attack (MinRank Attack)	Reducing HFE key recovery to solving a MinRank problem	Kipnis and Shamir (1999) [6]
MI	Linearization Attack	Directly solving using more equations than unknowns	Matsumoto and Imai (1988) [4], Patarin (1995) [5]
	Differential Attack	Using differential properties to recover structure	Fouque, Granboulan (2005) [66]
	MinRank-based Attack	Exploiting structure using low-	Kipnis and Shamir

Received: August 08 ,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Cryptosystem	Attack Name / Type	Description	Reference
		rank matrices	(1999) [6]
OV	Kipnis-Shamir Attack on OV	Exploiting rank properties of Oil-Vinegar mappings	Kipnis and Shamir (1999) [13]
	Albrecht-Cid Attack on Rainbow (OV Variant)	Exploiting the structure of Rainbow signatures	Albrecht and Cid (2021) [67]
	UOV (Unbalanced OV) Key Recovery Attack	Weaknesses due to imbalance between oil and vinegar variables	Kipnis et al. (1999) [13]
	Linearization Equations Attack (LEA)	Formulating linear equations for key recovery	Dubois et al. (2007) [68]

6. Conclusion

This study has presented a comprehensive review and comparative analysis of three foundational families of multivariate cryptosystems—HFE, Matsumoto-Imai, and Oil-Vinegar—highlighting their underlying algebraic structures, design principles, cryptographic strengths, and vulnerabilities. Each of these schemes reflects a unique approach to leveraging multivariate quadratic equations as a basis for public key cryptography, with varying degrees of success in terms of efficiency, key size, and resistance to cryptanalytic attacks.

The HFE scheme demonstrates strong theoretical design with high resistance to generic attacks, yet remains vulnerable to structural cryptanalysis without proper modifications. The MI cryptosystem, while elegant in its construction, has seen limited adoption due to practical vulnerabilities and its susceptibility to linearization attacks. The OV scheme, and especially its derivatives like Rainbow, has shown notable promise in digital signature applications, though recent cryptanalytic developments particularly during the NIST PQC standardization process have raised concerns regarding its long-term viability.

Through this triadic analysis, it becomes clear that while no single scheme offers a perfect balance of efficiency and security, the insights gained from each contribute significantly to the ongoing development of robust post-quantum cryptographic solutions.

7. Future Directions

Despite the progress made, the field of Multivariate Public Key Cryptography continues to face several open challenges and research opportunities:

Design of Hybrid and Variant Schemes: Combining favorable aspects of HFE, MI, and OV into hybrid schemes may help balance security and performance. Exploring new trapdoor structures and masking techniques remains an active area of research.

Received: August 08 ,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Cryptanalysis and Security Assumptions: There is a need for more rigorous analysis under quantum models and the development of formal security proofs. This includes revisiting assumptions about the hardness of the MQ problem and refining parameters to resist evolving attacks.

Efficiency Improvements: Reducing key sizes and enhancing computation speed without compromising security remains crucial, especially for constrained environments such as IoT and embedded systems.

Post-NIST Standardization Exploration: With the NIST PQC process nearing maturity, the exploration of alternate schemes or second-round candidates—including refined variants of OV and HFE—is vital to ensure diversity and resilience in cryptographic portfolios.

Application-Specific Adaptations: Tailoring MPKC schemes to specific applications like block chain, secure messaging, and cloud environments can lead to optimized cryptographic protocols that balance practicality with post-quantum security.

As quantum computing edges closer to practical realization, it is imperative for the cryptographic community to deepen its understanding of multivariate schemes and continue to innovate upon their foundations. The legacy of HFE, MI, and OV not only shapes today's MPKC landscape but also informs the path forward in building a secure, quantum-resilient digital future.

References

[1] T. Matsumoto and H. Imai (1983), A Class of Asymmetric Crypto-Systems based on Polynomials over finite Rings, IEEE Intern. Symp. Inform. Theory, St. Jovite, Quebec, Canada, September 26–30, 1983, Abstracts of Papers, pp. 131–132.

[2] Delsarte, P., Desmedt, Y., Odlyzko, A., Piret, P. (1985). Fast Cryptanalysis of the Matsumoto-Imai Public Key Scheme. In: Beth, T., Cot, N., Ingemarsson, I. (eds) Advances in Cryptology. EUROCRYPT 1984. Lecture Notes in Computer Science, vol 209. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-39757-4_14

[3] Imai, H., Matsumoto, T. (1986). Algebraic methods for constructing asymmetric cryptosystems. In: Calmet, J. (eds) Algebraic Algorithms and Error-Correcting Codes. AAECC 1985. Lecture Notes in Computer Science, vol 229. Springer, Berlin, Heidelberg.https://doi.org/10.1007/3-540-16776-5_713

[4] Matsumoto, T., Imai, H. (1988). Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption. In: Barstow, D., et al. Advances in Cryptology — EUROCRYPT '88. EUROCRYPT 1988. Lecture Notes in Computer Science, vol 330. Springer, Berlin, Heidelberg.https://doi.org/10.1007/3-540-45961-8_39

[5] Patarin, J. (1996). Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms. In: Maurer, U. (eds) Advances in

Received: August 08 ,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Cryptology — EUROCRYPT '96. EUROCRYPT 1996. Lecture Notes in Computer Science, vol 1070. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-68339-9_4

[6] Kipnis, A., Shamir, A. (1999). Cryptanalysis of the HFE Public Key Cryptosystem by Relinearization. In: Wiener, M. (eds) Advances in Cryptology — CRYPTO' 99. CRYPTO 1999. Lecture Notes in Computer Science, vol 1666. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-48405-1_2.

[7] Patarin, J., Courtois, N., Goubin, L. (2001). QUARTZ, 128-Bit Long Digital Signatures. In: Naccache, D. (eds) Topics in Cryptology — CT-RSA 2001. CT-RSA 2001. Lecture Notes in Computer Science, vol 2020. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-45353-9_21

[8] Patarin, J. (1995). Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88. In: Coppersmith, D. (eds) Advances in Cryptology — CRYPT0' 95. CRYPTO 1995. Lecture Notes in Computer Science, vol 963. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-44750-4_20

[9] Patarin, Jacques. "Asymmetric Cryptography with a Hidden Monomial." Annual International Cryptology Conference (1996)

[10] Patarin, Jacques & Goubin, Louis & Courtois, Nicolas. (1998). $C^{-+*}$and HM: Variations Around Two Schemes of T. Matsumoto and H. Imai. 1514. 35-50. 10.1007/3-540-49649-1_4.

[11] J. Patarin, The Oil and Vinegar Signature Scheme, presented at the Dagstuhl Workshop on Cryptography, september 1997 (transparencies).

[12] A. Kipnis, A. Shamir, Cryptanalysis of the Oil and Vinegar Signature Scheme, Proceedings of CRYPTO'98, Springer, LNCS no1462, pp. 257-266.

[13] Kipnis, A., Patarin, J., Goubin, L. (1999). Unbalanced Oil and Vinegar Signature Schemes. In: Stern, J. (eds) Advances in Cryptology — EUROCRYPT '99. EUROCRYPT 1999. Lecture Notes in Computer Science, vol 1592. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-48910-X_15

[14] Ding, J., Schmidt, D. (2005). Rainbow, a New Multivariable Polynomial Signature Scheme. In: Ioannidis, J., Keromytis, A., Yung, M. (eds) Applied Cryptography and Network Security. ACNS 2005. Lecture Notes in Computer Science, vol 3531. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11496137_12

[15] Braeken, A., Wolf, C., Preneel, B. (2005). A Study of the Security of Unbalanced Oil and Vinegar Signature Schemes. In: Menezes, A. (eds) Topics in Cryptology – CT-RSA 2005. CT-RSA 2005. Lecture Notes in Computer Science, vol 3376. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-30574-3_4

[16] Wolf, Christopher & Preneel, Bart. (2004). Asymmetric Cryptography: Hidden Field Equations.. IACR Cryptology ePrint Archive. 2004. 72.

Received: August 08 ,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[17] Jean-Charles Faug`ere and Antoine Joux. Algebraic cryptanalysis of Hidden Field Equations (HFE) using gr¨obner bases. In Advances in Cryptology — CRYPTO 2003, volume 2729 of Lecture Notes in Computer Science, pages 44–60. Dan Boneh, editor, Springer, 2003.

[18] Wolf, Christopher & Preneel, Bart. (2005). Applications of Multivariate Quadratic Public Key Systems. 413-424.

[19] Jacques Patarin. Hidden Field Equations (HFE) and Isomorphisms of Polynomials (IP): two new families of asymmetric algorithms. In Advances in Cryptology — EUROCRYPT 1996, volume 1070 of Lecture Notes in Computer Science, pages 33–48. Ueli Maurer, editor, Springer, 1996. Extended Version: http: //www.minrank.org/hfe.pdf

[20] Chen, Chia-Hsin & Chen, Ming-Shing & Ding, Jintai & Werner, Fabian & Yang, Bo-Yin. (2008). Odd-Char Multivariate Hidden Field Equations. IACR Cryptology ePrint Archive. 2008. 543.

[21] Billet, O., Macario-Rat, G. (2009). Cryptanalysis of the Square Cryptosystems. In: Matsui, M. (eds) Advances in Cryptology – ASIACRYPT 2009. ASIACRYPT 2009. Lecture Notes in Computer Science, vol 5912. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-10366-7_27

[22] Patarin, J., Courtois, N., Goubin, L. (2001). FLASH, a Fast Multivariate Signature Algorithm. In: Naccache, D. (eds) Topics in Cryptology — CT-RSA 2001. CT-RSA 2001. Lecture Notes in Computer Science, vol 2020. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-45353-9_22

[23] Courtois, Nicolas & Goubin, Louis & Patarin, Jacques. (2003). SFLASHv3, a fast asymmetric signature scheme.. IACR Cryptology ePrint Archive. 2003. 211.

[24] Ding, Jintai. (2004). A New Variant of the Matsumoto-Imai Cryptosystem through Perturbation. 305-318. 10.1007/978-3-540-24632-9_22.

[25] J. Ding, J.E. Gower, Inoculating multivariate schemes against differential attacks, in PKC 2006. Lecture Notes in Computer Science, vol. 3958 (Springer, Heidelberg, 2006), pp. 290– 301

[26] Rosenthal, Joachim, and Jens Zumbrägel.(2009) "MI-TTM Cryptosystem.", University of Zurich.

[27] Ding, J., Schmidt, D. (2005). Rainbow, a New Multivariable Polynomial Signature Scheme. In: Ioannidis, J., Keromytis, A., Yung, M. (eds) Applied Cryptography and Network Security. ACNS 2005. Lecture Notes in Computer Science, vol 3531. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11496137_12

[28] Braeken, A., Wolf, C., Preneel, B. (2005). A Study of the Security of Unbalanced Oil and Vinegar Signature Schemes. In: Menezes, A. (eds) Topics in Cryptology – CT-

Received: August 08 ,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

RSA 2005. CT-RSA 2005. Lecture Notes in Computer Science, vol 3376. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-30574-3_4

[29] Petzoldt, A., Bulygin, S., Buchmann, J. (2010). CyclicRainbow – A Multivariate Signature Scheme with a Partially Cyclic Public Key. In: Gong, G., Gupta, K.C. (eds) Progress in Cryptology - INDOCRYPT 2010. INDOCRYPT 2010. Lecture Notes in Computer Science, vol 6498. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-17401-8_4

[30] Petzoldt, A., Bulygin, S., Buchmann, J.: A Multivariate Signature Scheme with a partially cyclic public key. In: Proceedings of SCC 2010, pp. 229–235 (2010)

[31] Bettale, L., Faugère, JC. & Perret, L. Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic. Des. Codes Cryptogr. 69, 1–52 (2013). https://doi.org/10.1007/s10623-012-9617-2

[32] Petzoldt, Albrecht & Chen, Ming-Shing & Yang, Bo-Yin & Tao, Chengdong & Ding, Jintai. (2015). Design Principles for HFEv- Based Multivariate Signature Schemes. 9452. 311-334. 10.1007/978-3-662-48797-6_14.

[33] Petzoldt, A., Chen, M., Ding, J. and Yang, B. (2017), HMFEv - An Efficient Multivariate Signature Scheme, PQCrypto 2017: The Eighth International Conference on Post-Quantum Cryptography, Utrecht, -1, [online], (Accessed September 11, 2024) http://doi.org/10.1007/978-3-319-59879-6

[34] Jacques Patarin and Gilles Macario-Rat and Maxime Bros and Eliane Koussa, Ultra-Short Multivariate Public Key Signatures, Cryptology {ePrint} Archive, Paper 2020/914, 2020.

[35] Cogliati, B., Macariot-Rat, G., Patarin, J., Varjabedian, P. (2024). State of the Art of HFE Variants. In: Saarinen, MJ., Smith-Tone, D. (eds) Post-Quantum Cryptography. PQCrypto 2024. Lecture Notes in Computer Science, vol 14772. Springer, Cham. https://doi.org/10.1007/978-3-031-62746-0_7

[36] Hashimoto, Yasufumi. (2018). High-rank attack on HMFEv. JSIAM Letters. 10. 21-24. 10.14495/jsiaml.10.21.

[37] Cabarcas, D., Smith-Tone, D., Verbel, J.A. (2017). Key Recovery Attack for ZHFE. In: Lange, T., Takagi, T. (eds) Post-Quantum Cryptography . PQCrypto 2017. Lecture Notes in Computer Science(), vol 10346. Springer, Cham. https://doi.org/10.1007/978-3-319-59879-6_17

[38] Zhang, W., Tan, C.H. (2015). MI-T-HFE, A New Multivariate Signature Scheme. In: Groth, J. (eds) Cryptography and Coding. IMACC 2015. Lecture Notes in Computer Science(), vol 9496. Springer, Cham. https://doi.org/10.1007/978-3-319-27239-9_3

[39] Chen, M., Yang, B., & Smith-Tone, D. (2015). PFLASH - Secure Asymmetric Signatures on Smart Cards.

Received: August 08 ,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[40] Smith, Daniel. (2021). New Practical Multivariate Signatures from a Nonlinear Modifier. 10.1007/978-3-030-81293-5_5.

[41] Cartor, R., Smith-Tone, D. (2019). EFLASH: A New Multivariate Encryption Scheme. In: Cid, C., Jacobson Jr., M. (eds) Selected Areas in Cryptography – SAC 2018. SAC 2018. Lecture Notes in Computer Science(), vol 11349. Springer, Cham. https://doi.org/10.1007/978-3-030-10970-7_13

[42] Sakumoto, K., Shirai, T., Hiwatari, H. (2011). On Provable Security of UOV and HFE Signature Schemes against Chosen-Message Attack. In: Yang, BY. (eds) Post-Quantum Cryptography. PQCrypto 2011. Lecture Notes in Computer Science, vol 7071. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-25405-5_5

[43] Yasuda, T., Sakurai, K., Takagi, T. (2012). Reducing the Key Size of Rainbow Using Non-commutative Rings. In: Dunkelman, O. (eds) Topics in Cryptology – CT-RSA 2012. CT-RSA 2012. Lecture Notes in Computer Science, vol 7178. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-27954-6_5

[44] Thomae, E. (2012). Quo Vadis Quaternion? Cryptanalysis of Rainbow over Non-commutative Rings. In: Visconti, I., De Prisco, R. (eds) Security and Cryptography for Networks. SCN 2012. Lecture Notes in Computer Science, vol 7485. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-32928-9_20

[45] Yasuda, T., Ding, J., Takagi, T., & Sakurai, K. (2013). A variant of rainbow with shorter secret key and faster signature generation. AsiaPKC '13.

[46] Yasuda, T., Takagi, T., Sakurai, K. (2014). Efficient Variant of Rainbow without Triangular Matrix Representation. In: Linawati, Mahendra, M.S., Neuhold, E.J., Tjoa, A.M., You, I. (eds) Information and Communication Technology. ICT-EurAsia 2014. Lecture Notes in Computer Science, vol 8407. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-55032-4_55

[47] Petzoldt, A., Bulygin, S. (2013). Linear Recurring Sequences for the UOV Key Generation Revisited. In: Kwon, T., Lee, MK., Kwon, D. (eds) Information Security and Cryptology – ICISC 2012. ICISC 2012. Lecture Notes in Computer Science, vol 7839. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-37682-5_31

[48] Yasuda, T., Takagi, T., & Sakurai, K. (2014). Efficient variant of Rainbow using sparse secret keys. J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl., 5, 3-13.

[49] Weiwei Cao, Lei Hu, Jintai Ding, and Zhijun Yin. 2011. Kipnis-shamir attack on unbalanced oil-vinegar scheme. In Proceedings of the 7th international conference on Information security practice and experience (ISPEC'11). Springer-Verlag, Berlin, Heidelberg, 168–180.

[50] Z. Peng and S. Tang, "Circulant Rainbow: A New Rainbow Variant With Shorter Private Key and Faster Signature Generation," in IEEE Access, vol. 5, pp. 11877-11886, 2017, doi: 10.1109/ACCESS.2017.2717279.

Received: August 08 ,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[51] Furue, H., Ikematsu, Y., Kiyomura, Y., Takagi, T. (2021). A New Variant of Unbalanced Oil and Vinegar Using Quotient Ring: QR-UOV. In: Tibouchi, M., Wang, H. (eds) Advances in Cryptology-ASIACRYPT 2021. ASIACRYPT 2021. Lecture Notes in Computer Science, vol 13093. Springer, Cham. https://doi.org/10.1007/978-3-030-92068-5_7

[52] Beullens, W., Preneel, B. (2017). Field Lifting for Smaller UOV Public Keys. In: Patra, A., Smart, N. (eds) Progress in Cryptology – INDOCRYPT 2017. INDOCRYPT 2017. Lecture Notes in Computer Science(), vol 10698. Springer, Cham. https://doi.org/10.1007/978-3-319-71667-1_12

[53] Ding, J., Zhang, Z., Deaton, J., Schmidt, K., & Vishakha, F. (2019). New Attacks on Lifted Unbalanced Oil Vinegar.

[54] Nie, X., Liu, B., Xiong, H., Lu, G. (2016). Cubic Unbalance Oil and Vinegar Signature Scheme. In: Lin, D., Wang, X., Yung, M. (eds) Information Security and Cryptology. Inscrypt 2015. Lecture Notes in Computer Science(), vol 9589. Springer, Cham. https://doi.org/10.1007/978-3-319-38898-4_3

[55] Mus, K., Islam, S., & Sunar, B. (2020). QuantumHammer: A Practical Hybrid Attack on the LUOV Signature Scheme. Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security.

[56] Furue, H., Ikematsu, Y., Kiyomura, Y., Takagi, T. (2021). A New Variant of Unbalanced Oil and Vinegar Using Quotient Ring: QR-UOV. In: Tibouchi, M., Wang, H. (eds) Advances in Cryptology – ASIACRYPT 2021. ASIACRYPT 2021. Lecture Notes in Computer Science(), vol 13093. Springer, Cham. https://doi.org/10.1007/978-3-030-92068-5_7

[57] Jintai Ding, Joshua Deaton, Kurt Schmidt, Vishakha, and Zheng Zhang. 2020. Cryptanalysis of the Lifted Unbalanced Oil Vinegar Signature Scheme. In Advances in Cryptology – CRYPTO 2020: 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17–21, 2020, Proceedings, Part III. Springer-Verlag, Berlin, Heidelberg, 279–298. https://doi.org/10.1007/978-3-030-56877-1_10

[58] Beullens, W. (2022). Breaking Rainbow Takes a Weekend on a Laptop. In: Dodis, Y., Shrimpton, T. (eds) Advances in Cryptology – CRYPTO 2022. CRYPTO 2022. Lecture Notes in Computer Science, vol 13508. Springer, Cham. https://doi.org/10.1007/978-3-031-15979-4_16

[59] Ganguly, A., & Saxena, N. (2023). A New Multivariate Digital-Signature Scheme by Mixing Oil-Vinegar with Triangles.

[60] Ding, J., et al.: TUOV: Triangular Unbalanced Oil and Vinegar - Algorithm Specifications and Supporting Documentation Version 1.0. Round 1 Additional Signatures, Post-Quantum Cryptography: Digital Signature Schemes (2023).c

Received: August 08 ,2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[61] Hiroki Furue, Yutaro Kiyomura, Tatsuya Nagasawa, and Tsuyoshi Takagi. 2022. A New Fault Attack on UOV Multivariate Signature Scheme. In Post-Quantum Cryptography: 13th International Workshop, PQCrypto 2022, Virtual Event, September 28–30, 2022, Proceedings. Springer-Verlag, Berlin, Heidelberg, 124–143. https://doi.org/10.1007/978-3-031-17234-2_7

[62] Ganguly, A., Karmakar, A., Saxena, N. (2024). VDOO: A Short, Fast, Post-quantum Multivariate Digital Signature Scheme. In: Chattopadhyay, A., Bhasin, S., Picek, S., Rebeiro, C. (eds) Progress in Cryptology – INDOCRYPT 2023. INDOCRYPT 2023. Lecture Notes in Computer Science, vol 14460. Springer, Cham. https://doi.org/10.1007/978-3-031-56235-8_10

[63] Suparna Kundu and Quinten Norga and Uttam Kumar Ojha and Anindya Ganguly and Angshuman Karmakar and Ingrid Verbauwhede,mUOV: Masking the Unbalanced Oil and Vinegar Digital Sigital Signature Scheme at First- and Higher-Order, Cryptology ePrint Archive, Paper 2024/1875,2024.

[64] Gupta, A.J., Kumar, S., Biswal, S.K. (2025). Salted Cubic Unbalanced Oil and Vinegar Digital Signature Scheme. In: Patel, M.K., Ashraf, M., Mahdou, N., Kim, H. (eds) Algebra and Its Applications. ICAA 2023. Springer Proceedings in Mathematics & Statistics, vol 474. Springer, Singapore. https://doi.org/10.1007/978-981-97-6798-4_13

[65] Faugère, J.C., et al. (2003). Algebraic Cryptanalysis of HFE using Gröbner bases. EUROCRYPT 2003.

[66] Fouque, P.A., and Granboulan, L. (2005). Multivariate Cryptosystems and Differential Immunity. CT-RSA 2005.

[67] Albrecht, M.R., and Cid, C. (2021). On the Cryptanalysis of the Rainbow Signature Scheme. PQCrypto 2021.

[68] Dubois, V., Fouque, P.A., Stern, J., and Shamir, A. (2007). Practical Cryptanalysis of SFLASH. EUROCRYPT 2007.

Received: August 08 ,2025