Kajian Matematika Skema Tanda Tangan *Rainbow* Berbasis Multivariat

Arbi Nur'aini Labibah[1)], Sa'aadah Sajjana Carita[2)]
(1) Badan Siber dan Sandi Negara, arbi.nuraini@bssn.go.id
(2) Rekayasa Kriptografi, Politeknik Siber dan Sandi Negara, ss.carita@poltekssn.ac.id

Abstrak

Skema tanda tangan Rainbow merupakan skema tanda tangan berbasis multivariat yang pertama kali diperkenalkan oleh Jintai Ding dan Dieter Schmidt pada tahun 2005, serta berhasil mencapai ronde 3 pada proyek standardisasi kriptografi post quantum NIST. Skema ini menerapkan penggunaan multilayer untuk meningkatkan efisiensi dari skema tanda tangan Unbalanced Oil and Vinegar (UOV). Skema tanda tangan Rainbow yang diikutsertakan merupakan hasil modifikasi dengan penambahan vektor biner salt r yang bertujuan untuk memenuhi klaim keamanan Existential Unforgeability-Chosen Message Attack (EUF-CMA). Pada penelitian ini, penulis melakukan pengkajian terhadap dasar dan karakteristik, serta analisis dari klaim keamanan EUF-CMA yang dimiliki oleh skema modifikasi tanda tangan rainbow. Skema tanda tangan Rainbow terbukti memenuhi keamanan EUF-CMA dan karakteristik authentic, not reusable, unalterable, serta cannot be repudiated. Namun, skema ini tidak terjamin memenuhi karakteristik unforgeable dikarenakan key recovery attack yang dilakukan Ward Beullens pada tahun 2022.

Kata kunci: EUF-CMA; kriptografi multivariat; Oil and Vinegar; tanda tangan Rainbow; post quantum

Abstract

Rainbow signature scheme is a multivariate-based signature scheme first introduced by Jintai Ding and Dieter Schmidt in 2005, and reached the round 3 stage of the NIST post quantum cryptography standardization project. This scheme applies multilayer usage to improve the efficiency of the Unbalanced Oil and Vinegar (UOV) signature scheme. The Rainbow signature scheme submitted to the project is modified by the addition of a binary salt vector r to fulfill the keamanan Existential Unforgeability-Chosen Message Attack (EUF-CMA) security claim. The crucial status as a round 3 finalist makes many researchers perform attacks on the scheme. One of them is an attack carried out by Ward Beullens in 2022 by applying a key recovery attack which causes its security to not be guaranteed. In this research, we carried out a mathematical study of the basic, characteristics, and analysis of the EUF-CMA security claims of the rainbow signature modification scheme. The Rainbow signature scheme is proven to satisfy EUF-CMA security and authentic, not reusable, unalterable, and cannot be repudiated characteristics. Nevertheless, this scheme cannot be guaranteed to satisfy an unforgeable characteristic due to a private recovery attack by Ward Buellens in 2022.

Keywords: EUF-CMA; multivariate cryptography; Oil and Vinegar; Rainbow digital signature; post quantum

1. PENDAHULUAN

Teknologi informasi dan komunikasi yang menjadi salah satu pilar kehidupan era ini memerlukan pengamanan, di antaranya dengan kriptografi [1]. Kriptografi adalah ilmu terkait penyembunyian pesan dan banyak digunakan untuk melindungi data pada suatu sistem komputer atau jalur komunikasi. Sebagai contoh, kriptografi digunakan sebagai alat autentikasi dan enkripsi (e-mail dan kartu ATM), kontrol akses (pengamanan suatu fasilitas), proses pembayaran elektronik (*electronic cash*), dan sistem *e-voting* [2]. Berdasarkan penggunaan kuncinya, kriptografi dibedaan menjadi kriptografi simetris dan asimetris. Kriptografi kunci simetris menggunakan kunci yang sama untuk proses enkripsi dan dekripsinya, sedangkan kiptografi asimetris menggunakan dua kunci berbeda: kunci publik untuk enkripsi dan kunci privat untuk dekripsi [3], [4].

Perkembangan teknologi, termasuk komputer kuantum, membawa manfaat sekaligus ancaman bagi kriptografi. Pada tahun 1994, Peter Shor menyebutkan bahwa komputer kuantum memiliki kemampuan untuk memecahkan masalah faktorisasi bilangan bulat besar (*large integer factorization*) dan masalah logaritma diskrit (*discrete logarithm problem*), yang banyak digunakan pada kriptografi asimetris, dengan metode yang lebih cepat secara eksponensial menggunakan algoritma Shor [5], [6]. Untuk mengatasi permasalahan tersebut, pada Desember 2016, *National Institute of Standards and Technology* (NIST) mengumumkan proyek standardisasi kriptografi *post quantum* [6].

Proyek tersebut bertujuan menghasilkan standar algoritma *Key Encapsulation Mechanism* (KEM) dan tanda tangan digital. NIST menyebutkan beberapa properti keamanan yang harus dipenuhi oleh skema kriptografi yang akan distandarkan [7], diantaranya tahan terhadap *existential unforgeability – chosen message attack* (EUF-CMA) untuk skema tanda tangan. EUF-CMA merupakan suatu kondisi penyerang yang dapat melakukan pemalsuan tanda tangan dengan melakukan percobaan pada *signing oracle* [8]. Salah satu skema yang memenuhi

keamanan EUF-CMA adalah Rainbow [9].

Rainbow merupakan satu-satunya skema tanda tangan berbasis multivariat yang terpilih sebagai salah satu finalis pada ronde 3 standardisasi *kriptografi post quantum* di NIST. Skema ini dikembangkan dari tahun 2005 oleh Jintai Ding dan Dieter Schmidt. Skema Rainbow merupakan generalisasi dari konstruksi *Oil and Vinegar* untuk meningkatkan efisiensi dari skema tanda tangan *unbalanced Oil and Vinegar* [10]. Meskipun gugur pada ronde tersebut oleh serangan Ward Bullens [11] pada tahun 2022, pembelajaran mengenai strukturnya bermanfaat untuk desain skema tanda tangan *post quantum* berbasis multivariat di masa depan.

Penelitian ini melakukan kajian matematis skema tanda tangan Rainbow. Pengkajian yang dilakukan terkait karakteristik yang membangun skema modifikasi tanda tangan rainbow serta analisis dari klaim keamanan EUF-CMA.

2. LANDASAN TEORI

Berikut diberikan penjelasan singkat mengenai teori yang mendukung penelitian, yakni terkait transformasi Affine, kriptografi multivariat, skema *Oil and Vinegar*, dan EUF-CMA.

2.1 Transformasi Affine

Transformasi Affine pada $\mathbb{R}^n$ merupakan pemetaan $Aff : \mathbb{F}^n \to \mathbb{F}^n$ dengan bentuk

$$Aff(\mathbf{x}) = A \cdot \mathbf{x} + \boldsymbol{b}$$

untuk semua nilai $\mathbf{x} \in \mathbb{R}^n$, dengan A adalah matriks *invertible* pada $\mathbb{R}^n$.

Kata Affine memiliki arti adanya hubungan afinitas geometris yang kuat antara bentuk asli dan bentuk akhir setelah dilakukan perubahan [12]. Kolinearitas dan paralelisme adalah properti penting pada transformasi Affine [13]. Transformasi Affine dikatakan berkontraksi (*contracting*) jika jarak *euclidean* antara dua titik di bidang berkurang setelah kedua titik tersebut dipetakan oleh transformasi [14].

Dimisalkan transformasi Affine pada $F : \mathbb{F}^2 \to \mathbb{F}^2$, maka bentuk formulanya disajikan pada persamaan berikut:

$$Aff\left(\begin{bmatrix} x \\ y \end{bmatrix}\right) = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} e \\ f \end{bmatrix}, \quad (1)$$

dengan a, b, c, d, e, dan f adalah skalar [14].

2.2 Kriptografi Multivariat

Dasar dari kriptografi multivariat adalah sistem persamaan polinomial nonlinear dalam beberapa variabel pada *finite field* $\mathbb{F} = \mathbb{F}_q$ dengan q elemen, dituliskan pada persamaan (2) [16]:

$$\begin{aligned} p^{(1)}(x_1, \dots, x_n) &= \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij}^{(1)} . x_i x_j + \sum_{i=1}^{n} p_i^{(1)} . \ x_i \\ &\quad + p_0^{(1)} \\ &\vdots \\ p^{(2)}(x_1, \dots, x_n) &= \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij}^{(2)} . x_i x_j + \sum_{i=1}^{n} p_i^{(2)} . \ x_i \\ &\quad + p_0^{(2)} \\ &\vdots \\ p^{(m)}(x_1, \dots, x_n) &= \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij}^{(m)} . x_i x_j + \sum_{i=1}^{n} p_i^{(m)} . \ x_i \\ &\quad + p_0^{(m)} \end{aligned} \quad (2)$$

Keamanan dari skema kunci publik multivariat terletak pada kesulitan dalam penyelesaian sistem polinomial multivariat pada *finite fields* yang kemudian disebut sebagai permasalahan multivariat kuadrat (*Multivariat Quadratic*/MQ *problem*) [1], [15].

Definisi 2.1 MQ Problem [16]
Diberikan m polinomial kuadrat $p^{(1)}(\mathbf{x}), \dots, p^{(m)}(\mathbf{x})$ dengan n variabel $x_1, \dots, x_n$. Temukan vektor $\bar{\mathbf{x}} = (\bar{x}_1, \dots, \bar{x}_n)$ sehingga $p^{(1)}(\bar{\mathbf{x}}) = \cdots = p^{(m)}(\bar{\mathbf{x}}) = 0$.

Permasalahan pemecahan persamaan multivariat kuadrat pada m persamaan dengan n variabel terbukti sebagai permasalahan NP-*Complete* (*Nondeterministic Polinomial–time Complete*) [15], [17]. Meskipun dilakukan pemecahan permasalahan dengan komputer kuantum, permasalahan NP-*Complete* tetap sulit untuk diselesaikan dalam waktu polinomial. Oleh karena itu, kriptografi multivariat menjadi salah satu kandidat bagi kriptografi *post quantum*.

2.3 Skema *Oil and Vinegar*

Penjelasan mengenai skema ini diambil dari Sakumoto *et al.* [18]. Skema *oil* dan *vinegar* merupakan skema yang digunakan dalam pembangkitan sistem polinomial multivariat kuadrat *invertible* pada proses pembangkitan kunci. Skema ini pertama kali diajukan oleh Jacques Patarin pada tahun 1997. Dua jenis bilangan bulat digunakan sesuai dengan namanya, yaitu variabel *oil* yang dilambangkan sebagai o dan variabel *vinegar* dilambangkan sebagai v. Konsep yang diusung pada skema ini seperti halnya minyak dan cuka di mana keduanya tidak bercampur apabila disatukan dalam satu wadah.

Dimisalkan terdapat $\mathbb{F}$ yang merupakan *finite field*, o dan v yang merupakan dua buah bilangan bulat, dan n yang merupakan penjumlahan dari o dan v, $n = o + v$. Parameter yang digunakan oleh Patarin untuk menentukan nilai bilangan bulat o dan v pada awalnya adalah $o = v$ atau bernilai setara. Namun, pada tahun 1998, Kipnis dan Shamir berhasil memecahkan skema original dari Patarin tersebut. Untuk itu, pada tahun 1999, Kipnis, Patarin, dan Goubin mengajukan generalisasi dari skema "*oil and vinegar*" menjadi *Unbalanced Oil and Vinegar* (UOV)" yang menggunakan $v > o$ sebagai parameter untuk menentukan nilai bilangan bulat o dan v.

Dari himpunan $V = \{1, \dots, v\}$ dan $O = \{v +$

$1, \dots, n\}$, terdapat n variabel yang akan digunakan pada polinomial multivariat yang akan dibangkitkan yaitu $\{x_1, \dots, x_n\}$. Variabel tersebut yang sebelumnya disebut sebagai variabel *oil* dan *vinegar*. Himpunan $\{x_1, \dots, x_v\}$ merupakan variabel *vinegar* dan himpunan $\{x_{v+1}, \dots, x_n\}$ merupakan variabel *oil*. Persamaan (3) merupakan skema *oil* dan *vinegar* yang digunakan dalam konstruksi polinomial multivariat kuadrat, $f^{(k)}(\mathbf{x}) = f^{(k)}(x_1, \dots, x_n)$ dengan $(k \in O)$:

$$f^{(k)}(\mathbf{x}) = \sum_{i,j \in V, i \le j} \alpha_{ij}^{(k)} x_i x_j + \sum_{i \in V, j \in O} \beta_{ij}^{(k)} x_i x_j + \sum_{i \in V \cup O} \gamma_i^{(k)} x_i + \delta^{(k)} \quad (3)$$

2.4 EUF-CMA

Penerapan keamanan pada suatu tanda tangan memiliki tujuan untuk menghindari penyerang melakukan pemalsuan tanda tangan dari pasangan pesan dan tanda tangan, (m, σ) [2]. Pemalsuan tanda tangan terjadi saat penyerang mengetahui kunci privat dan memiliki akses secara keseluruhan pada *signing oracle*, $sign_{sk}(\cdot)$. *Signing oracle* ini akan bertindak sebagai *black box*. Penyerang dapat berinteraksi dengan *signing oracle* dengan mengirimkan input pesan pilihannya dan *signing oracle* akan mengirimkan *output* berupa tanda tangan yang valid (m^*, σ^*) kepada penyerang [8].

Existential Unforgeability (EUF) merupakan salah satu dari empat tingkat keamanan berdasarkan keberhasilan penyerang untuk memalsukan suatu tanda tangan [2]. Dimisalkan terdapat skema tanda tangan I yang terdiri dari tiga proses $(Gen, Sign, Verify)$. Algoritma 1 menjelaskan eksperimen dari EUF-CMA.

Algoritma 1 [11] $Exp_{A,I}^{euf-cma}(1^n)$

1. Bangkitkan $(sk, pk) \leftarrow Gen(1^n)$.
2. Penyerang A memiliki pk dan memiliki akses ke *signing oracle*, $Sign_{sk}(\cdot)$. Penyerang memberikan beberapa pesan $\{m^i\}_{i-1}^q$ kepada *oracle* untuk ditandatangani dengan sk, $A^{Sign_{sk}(\cdot)}(pk)$. Himpunan $\{m^i\}_{i-1}^q$ merupakan himpunan pesan yang dikirimkan penyerang kepada *oracle*.
3. *Oracle* akan menghasilkan $(m^*, \sigma^*) \leftarrow A^{Sign_{sk}(\cdot)}(pk)$.
4. Penyerang A dikatakan sukses apabila $Verify_{pk}(m^*, \sigma^*) = 1$ dan $m^* \notin \{m^i\}_{i-1}^q$.

3. METODE PENELITIAN

Penelitian ini termasuk dalam penelitian kualitatif yang dilakukan dengan telaah kepustakaan dan kajian matematis. Telaah kepustakaan dilakukan dengan mengumpulkan referensi dan teori yang berkaitan dari berbagai sumber, seperti buku, artikel, *paper*, atau jurnal. Konsep-konsep yang akan dibahas pada kajian matematis dipelajari dalam tahap ini, termasuk yang disajikan dalam Landasan Teori di atas.

Kajian matematis dilakukan dengan mempelajari dan membuktikan secara teoritis dasar materi dan karakteristik dari skema Rainbow serta penerapan dengan perhitungan sederhana untuk melihat cara kerjanya. Selanjutnya, dilakukan pembuktian dari klaim keamanan EUF-CMA yang diwajibkan oleh NIST. Hasil dari penelitian kemudian dituliskan dalam kesimpulan.

4. HASIL DAN PEMBAHASAN

Berikut akan diberikan penjelasan mengenai skema tanda tangan Rainbow, kajian mengenai konsep pembangunnya yakni konstruksi bipolar, serta modifikasi yang dilakukan agar memenuhi keamanan EUF-CMA. Selanjutnya akan dibuktikan ketepatan proses verifikasi dan pemenuhan klaim EUF-CMA tersebut. Analisis mengenai karakteristik serta penerapan dengan contoh parameter sederhana juga dilaksanakan.

4.1 Skema Tanda Tangan Rainbow

Penjelasan skema ini sesuai dengan [9]. Pada skema tanda tangan UOV, digunakan hanya satu *layer* $\ell = 1$, sedangkan pada skema tanda tangan *Rainbow* didefinisikan dengan beberapa *layer*. Penggunaan *layer* $\ell = 2$ membuat skema *rainbow* lebih efisien dan berukuran kunci yang lebih kecil, sedangkan penggunaan *layer* $\ell > 2$ menghasilkan ukuran kunci yang lebih besar pada level keamanan yang sama.

Skema yang akan disajikan merupakan skema modifikasi tanda tangan *Rainbow* yang diajukan oleh Jintai Ding *et al.* pada proyek standardisasi NIST. Perbedaan skema tanda tangan *Rainbow* original dan modifikasi terletak pada penggunaan vektor biner *salt* r. Berikut disajikan letak penambahan vektor biner *salt* r:

- Pertama, pada pembangkitan kunci, dilakukan penambahan nilai i, yang merupakan panjang dari vektor biner *salt* r, pada hasil akhir kunci publik $(\mathcal{P}, i)$ dan kunci privat $(InvS, c_S, \mathcal{F}, InvT, c_T, i)$.
- Kedua, pada proses pembangkitan tanda tangan dan verifikasi, nilai *hash* dari dokumen akan di-*concate* dengan vektor biner *salt* r, dengan semula nilai $\mathbf{h} = \boldsymbol{\mathcal{H}}(d)$ merupakan hasil nilai *hash* hanya dari dokumen. Kemudian, penambahan vektor biner *salt* r pada perhitungan nilai *hash* dokumen menjadi $\boldsymbol{h} = \boldsymbol{\mathcal{H}}(\boldsymbol{\mathcal{H}}(d)||r)$.
- Ketiga, nilai vektor biner *salt* r ditambahkan pada hasil dari pembangkitan tanda tangan, sehingga menjadi $\sigma = (\mathbf{z}, r)$.

Berikut disajikan parameter dan skema tanda tangan yang memiliki struktur seperti pada umumnya, yaitu pembangkitan kunci, tanda tangan, dan verifikasi.

4.1.1 Parameter

Berikut dirinci parameter-parameter yang digunakan pada skema tanda tangan *rainbow*:

- *Finite field* $\mathbb{F} = \mathbb{F}_q$ dengan q elemen
- Bilangan bulat $n = 0 < v_1 < \cdots < v_u < v_{u+1}$
- Himpunan $V_i = \{1, \dots, v_i\}$, $O_i = \{v_i + 1, \dots, V_{i+1}\}$ $(i = 1, \dots, \ell)$, sehingga untuk setiap $k \in O_i$.
- $|V_i| = v_i$ dan $|O_i| = o_i (i = 1, \dots, \ell)$
- Banyak persamaan dilambangkan sebagai m, $m = n - v_i$
- Banyak variabel dilambangkan sebagai n
- Vektor biner acak r (disebut sebagai *salt*)
- Panjang vektor biner acak r dinotasikan dengan i

4.1.2 Pembangkitan Kunci

Proses pembangkitan kunci menghasilkan sepasang kunci, yaitu kunci publik dan kunci privat, yang diberikan pada Algoritma 2.

Algoritma 2 *Key Generation*

Input: Parameter *rainbow* (q, v_1, o_1, o_2), i merupakan panjang dari vektor biner acak *salt* r.
Output: Pasangan kunci *rainbow* (sk, pk).

1. Tentukan parameter *rainbow* (q, v_1, o_1, o_2) yang digunakan.
2. Tentukan nilai dari i yang merupakan panjang dari vektor biner *salt* r.
3. Hitung $m = o_1 + o_2$, m merupakan banyak polinomial.
4. Hitung $n = m + v_1$, n merupakan banyak variabel.
5. Tentukan matriks $M_{\mathcal{S}} = Matriks(q, m, m)$ pada $\mathbb{F}_q$. Apabila matriks $M_{\mathcal{S}}$ tidak *invertible*, maka bangkitkan kembali matriks $M_{\mathcal{S}}$.
6. Hitung invers dari matriks $M_{\mathcal{S}}$, $Inv\mathcal{S} = M_{\mathcal{S}}^{-1}$.
7. Pilih nilai vektor $\boldsymbol{c_{\mathcal{S}}}$ berukuran m pada $\mathbb{F}_q$.
8. Lakukan pemetaan Affine dengan *input* $Aff(M_{\mathcal{S}}, \boldsymbol{c_{\mathcal{S}}})$, sehingga akan dihasilkan $\mathcal{S}: \mathbb{F}^m \to \mathbb{F}^m$ sebagai hasil pemetaan Affine.
9. Tentukan matriks $M_{\mathcal{T}} = Matriks(q, n, n)$ pada $\mathbb{F}_q$. Lakukan hal yang sama pada $M_{\mathcal{T}}$ sesuai langkah 5 hingga 8, sehingga akan didapatkan nilai dari vektor $\boldsymbol{c_{\mathcal{T}}}$ berukuran n pada $\mathbb{F}_q$ dan $\mathcal{T}: \mathbb{F}^n \to \mathbb{F}^n$ yang merupakan hasil pemetaan Affine dengan input $Aff(M_{\mathcal{T}}, \boldsymbol{c_{\mathcal{T}}})$.
10. Bangkitkan *central map* $\mathcal{F}$ dengan parameter yang sudah ditentukan sebelumnya, $Rainbowmap(q, v_1, o_1, o_2)$.
11. Lakukan pemetaan komposisi $\mathcal{S} \circ \mathcal{F} \circ \mathcal{T}$ untuk menghasilkan kunci publik $\mathcal{P}$.
12. Didapatkan pasangan kunci, yaitu kunci publik, $pk = (\mathcal{P}, i)$ dan kunci privat, $sk = (InvS, \boldsymbol{c_{\mathcal{S}}}, \mathcal{F}, InvT, \boldsymbol{c_{\mathcal{T}}}, i)$.

Berikut penjelasan tambahan dari Algoritma 2:

- $Matriks(q, m, m)$ adalah matriks berukuran $m \times m$ dengan koefisien yang dipilih secara acak pada $\mathbb{F}_q$.
- $Aff(M, \boldsymbol{c})$ adalah pemetaan Affine dengan bentuk $Aff(M, \boldsymbol{c}) = M \,.\, x + \boldsymbol{c}$.
- $Rainbowmap(q, v_1, o_1, o_2)$ adalah *central map* yang didasarkan pada parameter (q, v_1, o_1, o_2). Selain itu, koefisien $\alpha_{ij}^{(k)}, \beta_{ij}^{(k)}, \gamma_i^{(k)}$, dan $\delta^{(k)}$ dipilih secara acak pada $\mathbb{F}_q$.

Central map $\mathcal{F}$ merupakan fungsi $\mathcal{F}$ yang akan membangkitkan polinomial multivariat kuadrat yang dalam hal ini akan dibangkitkan dengan menerapkan skema *oil* dan *vinegar*. Persamaan (4) merupakan konstruksi *central map* $\mathcal{F}$ yang digunakan pada *Rainbow*:

$$\mathcal{F} = (f^{(v_1+1)}(\mathbf{x}), \dots, f^{(n)}(\mathbf{x}))$$

$$f^{(k)}(\mathbf{x}) = \sum_{i,j \in V_\ell, i \le j} \alpha_{ij}^{(k)} x_i x_j + \sum_{i \in V_\ell, j \in O_\ell} \beta_{ij}^{(k)} x_i x_j + \sum_{i \in V_\ell \cup O_\ell} \gamma_i^{(k)} x_i + \delta^{(k)} \qquad (4)$$

dengan $k \in O_\ell$ dan $\ell \in \{1, 2\}$.

Untuk *layer* pertama berlaku $V_1 = \{1, \dots, v_1\}$ dan $O_1 = \{v_1 + 1, \dots, v_1 + o_1\}$, sedangkan untuk *layer* kedua berlaku $V_2 = \{1, \dots, v_2 = v_1 + o_1\}$ dan $O_2 = \{v_2 + 1, \dots, n = v_2 + o_2\}$. Ketentuan tersebut akan digunakan sebagai input untuk membangkitkan polinomial multivariat kuadrat $f^{(k)}(\mathbf{x})$ sehingga akan dihasilkan $n - (v_1 + 1)$ polinomial untuk *central map* $\mathcal{F}$.

4.1.3 Pembangkitan Tanda Tangan

Algoritma 3 menghasilkan output nilai tanda tangan $\mathbf{z}$ dan akan dikirimkan kepada entitas lain bersamaan dengan nilai vektor biner *salt* r, sehingga menjadi sepasang nilai akhir tanda tangan $\sigma = (\mathbf{z}, r)$.

Algoritma 3 Pembangkitan Tanda Tangan

Input: Kunci privat *rainbow* $(InvS, c_{\mathcal{S}}, \mathcal{F}, InvT, c_{\mathcal{T}}, i)$, dokumen d, i merupakan panjang dari vektor biner *salt* r.
Output: hasil tanda tangan $(\boldsymbol{z}, r) \in \mathbb{F}^n \times \{0,1\}^i$ dengan $\mathcal{P}(\boldsymbol{z}) = \boldsymbol{\mathcal{H}}(\boldsymbol{\mathcal{H}}(d)||r)$

1. Bangkitkan:
   a. $(y_1, \dots, y_{v_1}) \in \mathbb{F}_q$.
   b. $\hat{f}^{(v_1+1)}, \dots, \hat{f}^{(n)} = f^{(v_1+1)}(y_1, \dots, y_{v_1}), \dots, f^{(n)}(y_1, \dots, y_{v_1})$
   c. $(\hat{F}, \boldsymbol{c_F}) = Aff^{-1}(\hat{f}^{(v_1+1)}, \dots, \hat{f}^{(n)})$

   Apabila $\hat{F}$ tidak *invertible*, maka lakukan kembali pemilihan nilai $(y_1, \dots, y_{v_1})$.
2. Hitung invers dari matriks $\hat{F}$, $InvF = \hat{F}^{-1}$.
3. Bangkitkan:
   a. Pilih nilai vektor biner *salt* $r \in \{0,1\}^i$ yang berukuran i.

b. Hitung $\mathbf{h} = \boldsymbol{\mathcal{H}}(\boldsymbol{\mathcal{H}}(d)||r)$, dengan fungsi *hash* $\boldsymbol{\mathcal{H}}$.
c. Hitung nilai $\mathbf{x} = InvS\ .\ (\mathbf{h} - \boldsymbol{c_S})$
d. $\left(y_{v_1+1}, \dots, y_{v_2}\right) = InvF \cdot \left(\left(x_{v_1+1}, \dots, x_{v_2}\right) - \boldsymbol{c_F}\right)$
e. $\hat{f}^{(v_2+1)}, \dots, \hat{f}^{(n)} = \hat{f}^{(v_2+1)}\left(y_{v_1+1}, \dots, y_{v_2}\right), \dots, \hat{f}^{(n)}(y_{v_1+1}, \dots, y_{v_2})$
f. Untuk mencari nilai $\left(y_{v_2+1}, \dots, y_n\right)$, lakukan eliminasi Gauss dari persamaan $(\hat{f}^{(v_2+1)} = x_{v_2+1}, \dots, \hat{f}^{(n)} = x_n)$.
g. Ulangi langkah 3, apabila hasil eliminasi Gauss menunjukkan persamaan tidak memiliki solusi.

4. Hitung $\mathbf{z} = InvT\ .\ (\mathbf{y} - \boldsymbol{c_T})$
5. Didapatkan pasangan nilai akhir tanda tangan sebagai berikut $\sigma = (\mathbf{z}, r)$

Pada Algoritma 3, digunakan fungsi *hash* $\boldsymbol{\mathcal{H}}: \{0,1\} \rightarrow \mathbb{F}^m$ untuk menghitung nilai *hash* $\mathbf{h} = \boldsymbol{\mathcal{H}}(\boldsymbol{\mathcal{H}}(d)||r) \in \mathbb{F}^m$.

4.1.4 Verifikasi

Algoritma 4 dilakukan dengan dua langkah: menghitung nilai hash dari dokumen dan substitusi nilai dari hasil pembangkitan tanda tangan, yaitu **z** ke kunci publik $\mathcal{P}$.

Algoritma 4 Verifikasi Tanda Tangan

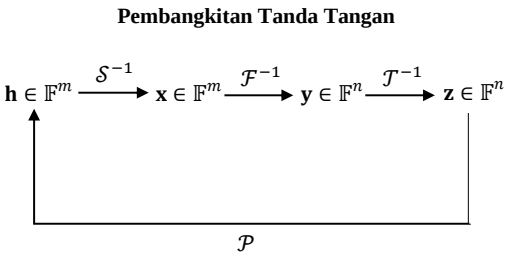
Input: dokumen d, tanda tangan $\sigma = (\mathbf{z}, r) \in \mathbb{F}^n \times \{0,1\}^i$
Output: hasil verifikasi tanda tangan valid atau ditolak.

1. Hitung $\mathbf{h} = \boldsymbol{\mathcal{H}}(\boldsymbol{\mathcal{H}}(d)||r)$, dengan fungsi *hash* $\boldsymbol{\mathcal{H}}$.
2. Hitung $\mathbf{h}' = \mathcal{P}(\mathbf{z}) \in \mathbb{F}^m$.
3. Jika $\mathbf{h}' = \mathbf{h}$, maka tanda tangan **z** diterima. Jika $\mathbf{h}' \neq \mathbf{h}$, maka tanda tangan **z** ditolak.

4.2 Konstruksi Bipolar

Konstruksi bipolar didasarkan dengan adanya *central map* $\mathcal{F}: \mathbb{F}^n \rightarrow \mathbb{F}^m$ yang terbentuk dari m polinomial multivariat kuadrat dengan n variabel yang memiliki invers, serta dua buah pemetaan Affine yang *invertible*, $\mathcal{S}: \mathbb{F}^m \rightarrow \mathbb{F}^m$ dan $\mathcal{T}: \mathbb{F}^n \rightarrow \mathbb{F}^n$. Penggunaan pemetaan Affine bertujuan untuk menyembunyikan struktur dari *central map* $\mathcal{F}$ sehingga menghasilkan suatu sistem polinomial baru $\mathcal{P}$ yang sulit untuk diinverskan. Dalam hal ini, konstruksi tersebut digunakan pada pembangkitan kunci publik $\mathcal{P}$, $\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}: \mathbb{F}^n \rightarrow \mathbb{F}^m$, sedangkan komponen pemetaan $\mathcal{S}$ dan $\mathcal{T}$, serta *central map* $\mathcal{F}$ akan disimpan sebagai kunci privat pengguna yang akan digunakan dalam proses pembangkitan tanda tangan. Alur konstruksi bipolar yang berlaku pada skema tanda tangan disajikan pada Gambar 1.

Dapat dilihat pada Gambar 1 bagaimana alur proses pembangkitan tanda tangan dan verifikasi yang berlaku pada skema tanda tangan *Rainbow*. Bentuk konstruksi bipolar memiliki dua permasalahan secara umum yang mendasari keamanannya, yaitu permasalahan *Multivariate Quadratic* (MQ) pada Definisi 2.1 dan permasalahan *Isomorphism of Polynomials* (IP). Permasalahan IP memiliki beberapa versi, salah satunya *Extended Isomorphism of Polynomials* (EIP) *problem* yang digunakan dalam skema Rainbow.



Gambar 1. Alur Konstruksi Bipolar

Definisi 4.1 Masalah EIP

Misal diberikan suatu sistem polinomial multivariat $\mathcal{P}$, dengan $\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}$ dengan $\mathcal{S}$ dan $\mathcal{T}$ sebagai pemetaan Affine/linear dan $\mathcal{F}$ yang merupakan sistem polinomial multivariat nonlinear. Tentukan dekomposisi dari $\mathcal{P}$, dengan $\mathcal{P} = \mathcal{S}' \circ \mathcal{F}' \circ \mathcal{T}'$ dengan $\mathcal{S}$ dan $\mathcal{T}$ sebagai pemetaan Affine atau linear, dan $\mathcal{F}'$. $\mathcal{F}'$ merupakan sistem polinomial multivariat nonlinear.

4.3 Pembuktian Verifikasi dan Klaim EUF-CMA

4.3.1 Pembuktian Verifikasi

Pada bagian ini akan disajikan pembuktian verifikasi dari skema tanda tangan *rainbow*. Suatu tanda tangan dikatakan valid saat hasil verifikasinya memenuhi kondisi $\boldsymbol{h} = \boldsymbol{h}'$, dengan $\boldsymbol{h} = \boldsymbol{\mathcal{H}}(\boldsymbol{\mathcal{H}}(d)||r)$ dan $h' = \mathcal{P}(\mathbf{z})$. Apabila hasil verifikasi tidak memenuhi kondisi tersebut, $\boldsymbol{h} \neq \boldsymbol{h}'$, maka tanda tangan dikatakan tidak valid. Berikut pembuktian verifikasi dari skema tanda tangan *Rainbow*:

$$\begin{aligned} \boldsymbol{h} &= \boldsymbol{h}' \\ \boldsymbol{\mathcal{H}}(\boldsymbol{\mathcal{H}}(d)||r) &= \mathcal{P}(\mathbf{z}) \\ &= (\mathcal{S} \circ \mathcal{F} \circ \mathcal{T})(\boldsymbol{z}) \\ &= \mathcal{S}\left(\mathcal{F}(\mathcal{T}(\mathbf{z}))\right), \end{aligned}$$

substitusi $\mathcal{T}(\mathbf{z}) = M_{\mathcal{T}} \cdot \mathbf{z} + C_{\mathcal{T}}$

$$\boldsymbol{\mathcal{H}}(\boldsymbol{\mathcal{H}}(d)||r) = \mathcal{S}(\mathcal{F}(M_{\mathcal{T}} \cdot \mathbf{z} + C_{\mathcal{T}})),$$

dengan $\mathbf{z} = InvT \cdot (\mathbf{y} - c_{\mathcal{T}})$ dan $InvT = M_{\mathcal{T}}^{-1}$

$$\begin{aligned} \boldsymbol{\mathcal{H}}(\boldsymbol{\mathcal{H}}(d)||r) &= \mathcal{S}\left(\mathcal{F}\left(M_{\mathcal{T}} \cdot \left(M_{\mathcal{T}}^{-1}\ .(\mathbf{y} - c_{\mathcal{T}})\right) + C_{\mathcal{T}}\right)\right) \\ &= \mathcal{S}(\mathcal{F}(\mathbf{y})), \text{ dengan } \mathcal{F}(\mathbf{y}) = \mathbf{x} \\ &= \mathcal{S}(\mathbf{x}) \\ &= M_{\mathcal{S}} \cdot \mathbf{x} + C_{\mathcal{S}}, \end{aligned}$$

dengan $\mathbf{x} = InvS\ \cdot\ (\mathbf{h} - c_{\mathcal{S}})$ dan $InvS = M_{\mathcal{S}}^{-1}$

$$\begin{aligned} &= M_{\mathcal{S}} \cdot \left(M_{\mathcal{S}}^{-1} \cdot (\mathbf{h} - c_{\mathcal{S}})\right) + C_{\mathcal{S}} \\ &= \mathbf{h} \end{aligned}$$

sehingga $\mathbf{h} = \mathbf{h}' = \boldsymbol{\mathcal{H}}(\boldsymbol{\mathcal{H}}(d)||r)$, dan disimpulkan

skema valid.

4.3.2 Pembuktian Keamanan EUF-CMA

Pembuktian ini berdasarkan penelitian Sakumoto *et al.* [18] kecuali disebutkan lain. Tidak diketahui secara pasti apakah skema tanda tangan UOV memenuhi EUF-CMA atau tidak, meskipun disebutkan menggunakan fungsi *trapdoor one-way*. Pada skema tanda tangan UOV dikatakan bahwa hasil tanda tangannya tidak terdistribusi secara seragam (*uniformly distributed*). Hal ini terjadi dikarenakan pada awal proses pembangkitan tanda tangan terdapat pemilihan satu himpunan variabel *vinegar*. Apabila solusi atau hasil tanda tangan belum ditemukan pada akhir proses pembangkitan tanda tangan, maka pengguna harus mengulang kembali proses tersebut dengan melakukan pemilihan ulang dari satu himpunan variabel *vinegar* hingga solusi akhir ditemukan. Hal ini membuat distribusi probabilitas dari satu himpunan variabel *vinegar* berubah seiring dengan banyaknya proses perulangan yang terjadi.

Probabilitas pemilihan himpunan variabel *vinegar* akan menjadi $> \frac{1}{q^v}$ seiring dengan adanya himpunan variabel *vinegar* terpilih yang tidak ditemukan solusinya. Oleh karena itu, tanda tangan yang dihasilkan pun tidak terdistribusi secara seragam. Suatu kejadian dikatakan terdistribusi secara seragam saat probabilitas kejadiannya seragam atau memiliki probabilitas yang sama meskipun dilakukan perulangan yang dalam hal ini seharusnya probabilitas pemilihan himpunan variabel *vinegar* adalah $\frac{1}{q^v}$. Hal yang sama berlaku pada skema tanda tangan *rainbow*, yang menerapkan skema *multilayer* UOV.

Berdasarkan [9], skema tanda tangan *Rainbow* yang diajukan pada proyek NIST memenuhi klaim keamanan EUF-CMA dengan menerapkan modifikasi yang sama seperti pada skema tanda tangan UOV. Modifikasi yang dilakukan adalah dengan penambahan vektor biner acak *salt* r yang berukuran i pada proses *hash* dari dokumen. Penambahan ini bersifat penambahan variabel baru dan tidak mengubah fungsi *trapdoor* yang ada. Apabila di akhir proses algoritma pembangkitan tanda tangan masih tidak ditemukan solusi, maka langkah yang harus diulang kembali adalah pemilihan nilai dari vektor biner acak *salt* r, sehingga himpunan variabel *vinegar* hanya dibangkitkan sekali di awal proses. Hal ini membuat variabel *vinegar* yang dibangkitkan terdistribusi secara seragam dengan probabilitas $\frac{1}{q^v}$, begitu juga hasil tanda tangan yang dihasilkan akan terdistribusi secara seragam.

Teorema 4.1 Jika suatu skema UOV memiliki parameter keamanan (ε', t'), maka skema modifikasi UOV memiliki parameter keamanan $(\varepsilon, t, q_H, q_s)$ dengan $\varepsilon = \frac{\varepsilon'(q_H+q_s+1)}{(1-(q_H+q_s)q_s.2^{-i})}$ dan $t = t' - (q_H + q_s + 1)(t_{UOV} + O(1))$, dengan t_{UOV} merupakan waktu komputasi yang diperlukan untuk menghitung kunci publik P.

Skema modifikasi tersebut memenuhi EUF-CMA dibuktikan dengan penerapan skenario pada *oracle*. Dalam hal ini, fungsi *hash* $\mathcal{H}$ akan bertindak sebagai *random oracle*. Jika i berukuran cukup besar, maka vektor acak *salt* r yang dibangkitkan akan *fresh* setiap saat dengan kemungkinan atau peluang yang besar. Dapat diibaratkan semakin besar i, maka peluang pemilihan satu vektor acak *salt* r akan semakin kecil dengan peluang sebesar $\frac{1}{2^i}$. Dengan demikian, $\mathbf{h}$ yang dihasilkan akan terdistribusi secara seragam (*uniformly distributed*) pada k^m, serta hasil tanda tangan ($\mathbf{z}$) yang dihasilkan akan juga terdistribusi secara seragam pada k^{m+v} dan vektor biner *salt* r dengan panjang i. Selain itu, *signing oracle* juga digunakan untuk penerapan skenario pada algoritma pembangkitan tanda tangan. Berikut skenario pemberian *challenge* pada *random oracle* dan *signing oracle*.

Skenario pemberian *challenge* pada *random oracle*: dimisalkan *challenge* yang diberikan pada *random oracle* B adalah $(m_i||r_i)$. Kondisi awal diketahui bahwa nilai L berisi kumpulan himpunan $(m_i, r_i, \cdot) \in L$, $i = 0$, dan $\alpha = \{1, \dots, q_H + q_s + 1\}$, dengan q_H merupakan *queries* atau permintaan yang diberikan pada *random oracle* dan q_s merupakan *queries* atau permintaan tanda tangan. Akan berlaku kondisi berikut.

1. Jika $i = 1$, maka B akan mengembalikan nilai acak $\mathbf{b} \in_R k^m$ sehingga terdapat himpunan $(m_i, r_i, \mathbf{b}) \in L$.
2. Jika $i = \alpha$, maka B akan mengembalikan nilai $\mathbf{h}$ sehingga $L = L \cup \{(m_i, r_i, \mathbf{h})\}$.
3. Jika $i > \alpha$, maka B akan mengembalikan nilai $\mathbf{b}_i$ sehingga $\mathbf{b}_i \in_R \mathbb{F}^n$ dan $L = L \cup \{(m_i, r_i, \mathbf{b}_i)\}$.

Skenario pemberian *challenge* pada *signing oracle*: dimisalkan *challenge* yang diberikan pada *signing oracle* adalah pesan m_i. *Oracle* akan memilih nilai $r_i \in_R \{0,1\}^i$ dan $z_i \in_R \mathbb{F}^{m+v}$, serta menghitung nilai dari $\mathbf{h} = P(\mathbf{z}_i)$. Apabila hasil tersebut sama, maka *oracle* akan mengembalikan nilai tanda tangan $\sigma = (\mathbf{z}_i, r_i)$.

Dalam hal ini, diasumsikan penyerang A melakukan skenario kepada *oracle*. Dengan demikian, penyerang A akan bisa menghasilkan suatu *forgery* hasil tanda tangan $(\mathbf{z}, r)$ untuk pesan apabila berhasil mendapatkan jawaban dari *oracle*, yaitu nilai $\mathbf{h}$. Apabila mendapatkan selain dari itu, maka proses *forgery* gagal dilakukan oleh penyerang A.

Hasil tanda tangan ($\mathbf{z}$) yang dihasilkan oleh algoritma pembangkitan tanda tangan akan terdistribusi secara seragam pada $\mathbb{F}^{m+v}$. Peluang dari kesuksesan penyerang dalam melakukan serangan menggunakan *oracle* disajikan pada persamaan (5):

$$\sum_{i=0}^{\infty} Pr\left[\begin{array}{c} x_v \in_R \mathbb{F}^v,\ H_1, \dots, H_i \in_R \mathbb{F}^m,\ x_m \in_R \{z_m | \mathcal{F}_{Rainbow}(z_m, x_v) = H_i\}; \\ \{z_m | \mathcal{F}_{Rainbow}(z_m, x_v) = H_1\} = \emptyset, \dots, \{z_m | \mathcal{F}_{Rainbow}(z_m, x_v) = H_{i-1}\} = \emptyset, \\ \{z_m | \mathcal{F}_{Rainbow}(z_m, x_v) = H_i\} \neq \emptyset,\ (x_m, x_v) = (x'_m, x'_v); \end{array}\right]$$

$$= \frac{1}{q^v} \cdot \frac{\Pr\left[\begin{array}{c} H \in_R \mathbb{F}^m,\ x_m \in_R \{z_m | \mathcal{F}_{Rainbow}(z_m, x_v) = H\}; \\ x_n \in_R \{z_m | \mathcal{F}_{Rainbow}(z_m, x_v) = H\} \neq \emptyset,\ x_n = x'_n; \end{array}\right]}{\Pr[H \in_R \mathbb{F}^m,\ x_m \in_R \{z_m | \mathcal{F}_{Rainbow}(z_m, x_v) = H\} \neq \emptyset :]} = \frac{1}{q^{m+v}},$$

dengan $m = o_1 + o_2$ (5)

4.4 Analisis Karakteristik

Suatu skema tanda tangan dikatakan layak digunakan apabila memenuhi lima karakteristik dasar skema tanda tangan [19], dengan penjelasan sebagai berikut:

a. Tanda tangan harus asli (*authentic*)
   Keaslian suatu tanda tangan dapat diperiksa dengan melihat pada proses verifikasinya. Apabila proses verifikasi berhasil, maka kepemilikan *file* tersebut sama dengan kepemilikan kunci publik yang digunakan oleh penerima.
   Hal ini dapat dilihat pada proses verifikasi *Rainbow* dilakukan dengan cara memastikan kondisi $\boldsymbol{h} = \boldsymbol{h}'$, dengan $\boldsymbol{h} = \boldsymbol{\mathcal{H}}(\boldsymbol{\mathcal{H}}(d)||r)$ dan $h' = \mathcal{P}(\mathbf{z})$. Hal ini juga dapat dilihat pada pembuktian verifikasi yang tercantum pada bagian 4.3.1. Selain itu, keaslian suatu tanda tangan juga dapat dipastikan dengan memanfaatkan penggunaan *certificate authority* (CA) yang dikeluarkan oleh pihak ketiga untuk memvalidasi identitas penandatangan pada dokumen.
b. Tanda tangan tidak dapat dipalsukan (*unforgeable*)
   Skema modifikasi tanda tangan *Rainbow* memenuhi klaim keamanan EUF-CMA seperti yang sudah dijelaskan pada bagian 4.3.2. Namun, pada tahun 2022, Ward Beullens dapat melakukan serangan *key recovery* pada kunci publiknya, sehingga kunci privat dapat dipecahkan. Jika kunci privat sudah dapat dipecahkan, maka pemalsuan tanda tangan juga dapat dilakukan. Hal ini menyebabkan skema modifikasi tanda tangan *rainbow* ini kembali diragukan keamanannya dan tidak memenuhi karakteristik ini.
c. Tanda tangan tidak dapat digunakan kembali (*not reusable*)
   Suatu nilai tanda tangan yang dihasilkan memiliki hubungan erat dengan nilai *hash* dari dokumen yang akan ditandatangani. Apabila suatu suatu tanda tangan digunakan kembali untuk dokumen lain dengan cara dipindahkan, maka hal tersebut akan terlihat pada proses verifikasi yang tidak valid.
   Sebagai contoh, terdapat dokumen A yang akan ditandatangani dengan tanda tangan *Rainbow* sehingga nilai tanda tangnannya adalah σ_A. Penyerang kemudian memindahkan tanda tangan tersebut ke dokumen B dan mengirimkannya (dokumen B dengan nilai tanda tangan σ_A) kepada penerima. Ini akan terlihat saat penerima akan melakukan proses verifikasi, di mana penerima akan memiliki nilai *hash* dari dokumen B dan nilai tanda tangan σ_A. Proses verifikasi tersebut akan menjadi tidak valid.
d. Dokumen yang ditandatangani tidak dapat diubah (*unalterable*)
   Apabila suatu dokumen diubah, meskipun hanya perubahan kecil seperti menambah satu huruf atau memberi *highlight*, maka nilai *hash* dari dokumen tersebut akan berubah. Hal ini akan mempengaruhi proses verifikasinya yang menjadi tidak valid karena nilai *hash* tersebut bukan dari dokumen aslinya.
   Sebagai contoh, terdapat dokumen A, d_A, yang sudah ditandatangani dengan nilai *hash* $\boldsymbol{\mathcal{H}}(d_A)$ dan dilakukan perubahan pada *file* tersebut sehingga nilai *hash* nya menjadi $\boldsymbol{\mathcal{H}}(d_A{}')$. Pada proses verifikasi, ditemukan kondisi $\boldsymbol{h} \neq \boldsymbol{h}'$ karena $\boldsymbol{h} = \boldsymbol{\mathcal{H}}(\boldsymbol{\mathcal{H}}(d_A{}')||r)$ dan $h' = \mathcal{P}(\mathbf{z})$, dengan $d_A{}'$ merupakan dokumen A yang sudah mengalami perubahan.
e. Tanda tangan tidak dapat disangkal (*cannot be repudiated*)
   Anti penyangkalan (*non-repudiation*) merupakan salah satu sifat yang harus dimiliki oleh tanda tangan digital. Dalam hal ini, skema modifikasi tanda tangan *rainbow* membangkitkan dua jenis kunci seperti skema tanda tangan pada umumnya, yaitu kunci publik dan kunci privat. Kunci publik tersebut akan dikirimkan kepada entitas lain yang berperan sebagai penerima, sedangkan kunci privatnya akan tetap dipegang oleh pengguna.
   Saat entitas lain menerima dokumen yang sudah ditandatangani, maka entitas tersebut dapat memastikan identitas pemiliknya. Pengguna atau pemilik tanda tangan tersebut tidak dapat menyangkalnya dikarenakan adanya identitas pemilik dan waktu penandatangannya.

5. KESIMPULAN

Berdasarkan hasil kajian dan analisis pada penelitian ini, disimpulkan bahwa permasalahan yang mendasari keamanan skema tanda tangan Rainbow ada dua yakni MQ (*Multivariate Quadratic*) dan EIP (*Extended Isomorphism of Polynomials*). Dari kelima karakteristik tanda tangan digital, skema ini memenuhi empat yaitu *authentic*, *not reusable*, *unalterable,* dan *cannot be repudiated.*

Skema tanda tangan Rainbow memenuhi klaim keamanan EUF-CMA (*Existential Unforgeability-*

Chosen Message Attack) melalui skenario *challenge-response* pada *signing oracle* dan *random oracle.* Meskipun demikian, *key recovery attack* yang dilakukan oleh Ward Beullens pada tahun 2022 berhasil mendapatkan kunci privat, sehingga dengan parameter yang diajukan pada proyek standardisasi NIST, skema ini tidak terjamin memenuhi salah satu karakteristik tanda tangan digital yaitu *unforgeable.*

Penulis mengajukan saran untuk pengembangan penelitian selanjutnya mengenai parameter yang dapat digunakan oleh skema tanda tangan Rainbow agar dapat tahan terhadap *key recovery attack*. Penelitian mengenai desain skema tanda tangan berbasis multivariat lain juga diperlukan agar dapat dijadikan salah satu standar algoritma *post quantum.*

REFERENSI

[1] V. Mavroeidis, K. Vishi, M. D., and A. Jøsang, "The Impact of Quantum Computing on Present Cryptography," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 3, pp. 405–414, 2018, doi: 10.14569/IJACSA.2018.090354.

[2] S. Vaudenay, *A Classical Introduction to Cryptography*. New York: Springer-Verlag, 2006.

[3] H. Xu, K. Thakur, A. S. Kamruzzaman, and M. L. Ali, "Applications of Cryptography in Database: A Review," in *2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, Apr. 2021, pp. 1–6, doi: 10.1109/IEMTRONICS52119.2021.9422663.

[4] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 2018.

[5] E. Grumbling and M. Horowitz, *Quantum Computing*, vol. 9781461418. Washington, D.C.: National Academies Press, 2019.

[6] A. Ferozpuri and K. Gaj, "High-speed FPGA Implementation of the NIST Round 1 Rainbow Signature Scheme," in *2018 International Conference on ReConFigurable Computing and FPGAs (ReConFig)*, Dec. 2018, no. 1, pp. 1–8, doi: 10.1109/RECONFIG.2018.8641734.

[7] NIST, "Proposed Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process," 2016. https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf.

[8] M. Jurkiewicz, "Improving Security of Existentially Unforgeable Signature Schemes," *Int. J. Electron. Telecommun.*, vol. 66, no. 3, pp. 473–480, Jan. 2020, doi: 10.24425/ijet.2020.131901.

[9] J. Ding *et al.*, "Rainbow Public Key : System of multivariate quadratic polynomials," 2021. https://csrc.nist.gov/CSRC/media/Presentations/rainbow-round-3-presentation/images-media/session-1-rainbow-petzoldt.pdf.

[10] J. Ding and D. Schmidt, "Rainbow, a New Multivariable Polynomial Signature Scheme," in *Lecture Notes in Computer Science*, vol. 3531, 2005, pp. 164–175.

[11] W. Beullens, "Breaking Rainbow Takes a Weekend on a Laptop," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 13508 LNCS, Springer Nature Switzerland, 2022, pp. 464–479.

[12] J. Vince, *Mathematics for Computer Graphics*. London: Springer London, 2010.

[13] M. E. Mortenson, *Mathematics for Computer Graphics Applications*, 2nd ed. New York, NY: Industrial Press, Inc.

[14] H. Anton and C. Rorres, *Elementary Linear Algebra*, 11th ed. Wiley.

[15] J. Ding and B.-Y. Yang, "Multivariate Public Key Cryptography," *Post-Quantum Cryptogr.*, no. 1, pp. 193–241, 2009, doi: 10.1007/978-3-540-88702-7_6.

[16] J. Ding and A. Petzoldt, "Current State of Multivariate Cryptography," *IEEE Secur. Priv.*, vol. 15, no. 4, pp. 28–36, 2017, doi: 10.1109/MSP.2017.3151328.

[17] W. J. Buchanan, "The Oil and Vinegar Method," no. September, 2020, doi: 10.6084/m9.figshare.13012016.v1.

[18] K. Sakumoto, T. Shirai, and H. Hiwatari, "On provable security of UOV and HFE signature schemes against chosen-message attack," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 7071 LNCS, pp. 68–82, 2011, doi: 10.1007/978-3-642-25405-5_5.

[19] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed. 1996.