cryptography

MDPI

Article

An Improved Identity-Based Multivariate Signature Scheme Based on Rainbow

Le Van Luyen

Faculty of Mathematics and Computer Science, University of Science, VNU-HCM, 227 Nguyen Van Cu, District 5, Ho Chi Minh City 72711, Vietnam; lvluyen@hcmus.edu.vn

Received: 19 January 2019; Accepted: 14 March 2019; Published: 17 March 2019

Abstract: Multivariate Public Key Cryptography (MPKC) is one of the main candidates for post-quantum cryptography, especially in the area of signature schemes. In this paper, we instantiate a certificate Identity-Based Signature (IBS) scheme based on Rainbow, one of the most efficient and secure multivariate signature schemes. In addition, we revise the previous identity-based signature scheme IBUOV based on the Unbalanced Oil and Vinegar (UOV) scheme on the security and choice of parameters and obtain that our scheme is more efficient than IBUOV in terms of key sizes and signature sizes.

Keywords: post-quantum cryptography; multivariate cryptography; UOV; rainbow; identity-based signature

1. Introduction

Post-quantum cryptography is a new direction in the last two decades after the thread of polynomial quantum algorithms of Shor [1], which totally broke the currently most widely-used public key cryptosystems such as RSA [2], DSA [3], and ECC [4]. It has received much more attention recently after the call of NIST [5] for proposals of post-quantum cryptosystems to be standardized in the near future. There have been a number of submissions for the first round [6], and the first NIST conference has been recently held for discussions [7].

Multivariate cryptography is one of the main candidates for this standardization [5,6]. These schemes are in general very fast and require only modest computational resources, which can be used on low-cost devices like smart cards and RFID chips [8,9]. Multivariate schemes were first proposed by Matsumoto and Imai in the mid-1980s [10]. Since then, there has been a rich development of designing multivariate schemes in several directions, e.g., BigField or SingleField schemes. The first SingleField signature scheme was the Oil and Vinegar (OV) signature scheme, introduced by Patarin after he broke the Matsumoto–Imai scheme [11]. Soon after, Patarin broke the OV schemes and introduced a variant [12], which is called the Unbalanced Oil and Vinegar (UOV) scheme. After around two decades, UOV schemes were still secure up to the choices of parameters. While the signature generation of UOV is very efficient, it has a very large public key. To deal with this, several improvements have been suggested. The first improvement was made by Ding and Schmidt [13], who proposed the Rainbow signature scheme, which can be seen as a multi-layer version of UOV with smaller keys and shorter signatures. The Rainbow signature scheme has remained secure for more than a decade and has been submitted as a candidate for the NIST standardization competition [6].

In practice, digital certificates linking public keys with identities of users are needed, and this fact leads to some drawbacks in efficiency and simplicity. For this reason, the alternative framework of identity-based cryptography was introduced by Shamir [14]. The idea is that the public key of a user can be directly derived from his/her identity, and therefore, digital certificates are avoidable. Shamir already proposed an Identity-Based Signature scheme (IBS), but it took a while until the first

identity-based encryption arrived [15]. In the area of multivariate cryptography, there has been only one proposal in the area of identity-based cryptography, that is the identity-based signature scheme IBUOV based on the UOV scheme [16]. However, the authors of IBUOV simply used the standard version of UOV, which is not Existential Unforgeability under Chosen-Message Attack (EU-CMA) secure. This implies that the constructed IBS scheme is also not EU-CMA secure. Moreover, they also proposed the wrong parameters with the corresponding desired security level, as well as computed the wrong the corresponding key sizes.

In this paper, we adapt the method of Shamir to instantiate an identity-based signature scheme based on a provable version of Rainbow, which we call IBS-Rainbow. Since our Rainbow scheme is EU-CMA secure, the resulting IBS-Rainbow is also EU-CMA secure. In addition, we also adapt a provable UOV scheme in [17] to IBUOV, revise the parameter choice for IBUOV, and compare with our IBS-Rainbow scheme. As a result, our IBS-Rainbow scheme is more efficient than IBUOV in terms of both key sizes and signature sizes.

The paper is organized as follows. We recall some definitions of digital signatures and identity-based signatures in Section 2. We also present the construction of an IBS scheme from a digital signature scheme. In Section 3, we present some basics of multivariate cryptography and recall the UOV and Rainbow schemes. Section 4 is devoted o the modified versions of UOV and Rainbow, which are proven to be EU-CMA secure. Attacks against Rainbow are also presented. In Section 5, we present the construction of our IBS-Rainbow scheme and the parameter choices. Section 6 concludes the paper.

2. Preliminaries

In this section, we first recall some basic notions on digital signatures and identity-based signatures and a transformation from a digital signature into an identity-based signature.

An *Identity-Based Signature* ($\mathcal{IBS}$) scheme is a tuple of polynomial-time algorithms $(\text{Setup}, \text{KeyDer}, \text{Sign}, \text{Vf})$. The first three are randomized, but the last one. The trusted key distribution center runs the setup algorithm Setup on input 1^k to obtain a master public and secret key (mpk, msk). To generate the secret signing key usk for the user with identity $id \in \{0,1\}^*$, it runs the key derivation algorithm KeyDer on inputs msk and id. On input usk and a message M, the signing algorithm Sign returns a signature σ of M. On inputs mpk, id, M, σ, the verification algorithm Vf returns one if σ is valid for id and M and returns zero otherwise. Correctness requires that $\text{Vf}(mpk, id, M, \sigma) = 1$ with a probability of one for all $k \in \mathbb{N}$ and id, M whenever the keys are generated as indicated above.

For security, we follow the notion of Existential Unforgeability under Chosen-Message and chosen-identity Attack (EU-CMA). It is defined through a game with a forger F and parameterized with the security parameter k. The experiments begin with the generation of a fresh master public and secret key pair (msk, msk). The forger F is run on the input of the master public key mpk and has access to the following oracles:

- $\text{KeyDer}(\cdot)$: on the input identity id, this oracle returns a secret signing key usk.
- $\text{Sign}(\cdot)$: on the input identity id and a message M, this oracle returns a signature $\sigma \leftarrow \text{Sign}(usk, M)$ where $usk \leftarrow \text{KeyDer}(msk, id)$.

At the end of its execution, the forger outputs identity id^*, message M^*, and a forged signature σ^*. The forger is said to win the game if $\text{Vf}(mpk, id^*, M^*, \sigma^*) = 1$ and F never queried $\text{KeyDer}(id^*)$ or $\text{Sign}(id^*, M^*)$. The advantage $\mathbf{Adv}^{\text{EU-CMA}}_{\mathcal{IBS},F}(k)$ is defined to be the probability that F wins the game, and $\mathcal{IBS}$ is said to be EU-CMA secure if $\mathbf{Adv}^{\text{EU-CMA}}_{\mathcal{IBS},F}(k)$ is negligible in k for all polynomial-time forgers F, i.e., for all $c \in \mathbb{N}$, there exists $k_c \in \mathbb{N}$ such that $\mathbf{Adv}^{\text{EU-CMA}}_{SS,F}(k) < k^{-c}$ for all $k > k_c$.

A *Standard Signature* ($\mathcal{SS}$) scheme consists of three polynomial-time algorithms $(\text{KeyGen}, \text{Sign}, \text{Vf})$. The randomized key generation algorithm KeyGen, on input 1^k, generates a key pair (pk, sk). The signer creates a signature on a message M via $\sigma \leftarrow \text{Sign}(sk, M)$, and the verifier

can check the validity of a signature σ by testing whether $\mathrm{Vf}(pk, M, \sigma) = 1$. It is required that for all messages M, $\mathrm{Vf}(pk, M, \sigma) = 1$ with a probability of one.

The security notion for a signature scheme $\mathcal{SS}$ is defined through the notion of EU-CMA, described as the following game with a forger F. The forger is run with a fresh public key pk as an input and is given access to a signing oracle for the corresponding secret key sk. It is said to win the game if it can output a pair (M^*, σ^*) such that $\mathrm{Vf}(pk, M^*, \sigma^*) = 1$ and it never queried M^* from the signing oracle. The advantage $\mathbf{Adv}^{\text{EU-CMA}}_{\mathcal{SS},F}(k)$ is defined as the probability that F wins this game. $\mathcal{SS}$ is said to be EU-CMA secure if $\mathbf{Adv}^{\text{EU-CMA}}_{\mathcal{SS},F}(k)$ is a negligible function in k for all polynomial-time forger F.

Given a standard signature scheme $\mathcal{SS} = (\mathrm{KeyGen}, \mathrm{Sign}, \mathrm{Vf})$, one can build a certificate-based IBS scheme $\mathcal{IBS} = (\mathrm{Setup}, \mathrm{KeyDer}, \mathrm{Sign}', \mathrm{Vf}')$ as the following.

Setup(1^k)**:** Run $\mathrm{KeyGen}(1^k)$ to obtain (mpk, msk).
KeyDer(msk, id)**:** $(pk, sk) \leftarrow \mathrm{KeyGen}(1^k)$, $cert \leftarrow \mathrm{Sign}(msk, pk \| id)$; and return $usk \leftarrow (sk, pk, cert)$.
Sign$'(usk, M)$**:** Parse usk as $(sk, pk, cert)$; compute $\sigma \leftarrow \mathrm{Sign}(sk, M)$; and return $\sigma' = (\sigma, pk, cert)$.
Vf$'(mpk, id, M, \sigma')$**:** Parse σ' as $(\sigma, pk, cert)$, and check if both $\mathrm{Vf}(pk, M, \sigma) = 1$ and $\mathrm{Vf}(mpk, pk \| id, cert) = 1$ are satisfied, then return one, otherwise zero.

One can see that if $\mathcal{SS}$ is EU-CMA, then the constructed $\mathcal{IBS}$ above is also EU-CMA; see [18] for more details and the references therein. In this paper, we will present a multivariate signature scheme that is EU-CMA and apply the above transformation to construct an EU-CMA-secure IBS scheme.

3. Multivariate Public Key Cryptography

In this section, we recall some basic concepts of multivariate public key cryptography. The basic objects of multivariate cryptography are systems of multivariate quadratic polynomials over a finite field K. The security of multivariate schemes is based on the *MQ-problem*, which asks for a solution of a given system of multivariate quadratic polynomials over the field K. The MQ-problem has been proven to be NP-hard even for quadratic polynomials over the field $\mathbb{F}_2$ [19].

To build a multivariate public key cryptosystem, one starts with an easily-invertible quadratic map $\mathcal{F} : K^n \to K^m$ (*central map*). To hide the structure of $\mathcal{F}$ in the public key, one composes it with two invertible affine (or linear) maps $\mathcal{T} : K^m \to K^m$ and $\mathcal{S} : K^n \to K^n$. The *public key* is therefore given by $\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S} : K^n \to K^m$. The *private key* consists of $\mathcal{T}, \mathcal{F}$ and $\mathcal{S}$.

In this paper, we consider multivariate signature schemes. For these schemes, we require $n \geq m$, which ensures that every message has a signature. The signature generation and verification are as the following, which is depicted in Figure 1.

Signature generation: To generate a signature for a message (or its hash value) $\mathbf{d} \in K^m$, one computes recursively $\mathbf{w} = \mathcal{T}^{-1}(\mathbf{d}) \in K^m$, $\mathbf{y} = \mathcal{F}^{-1}(\mathbf{w}) \in K^n$ and $\mathbf{z} = \mathcal{S}^{-1}(\mathbf{y})$. Then, $\mathbf{z} \in K^n$ is the signature of the message $\mathbf{d}$. Here, $\mathcal{F}^{-1}(\mathbf{w})$ means finding one (of possibly many) pre-image of $\mathbf{w}$ under the central map $\mathcal{F}$.

Signature verification: To check the authenticity of a signature $\mathbf{z} \in K^n$, the verifier simply computes $\mathbf{d}' = \mathcal{P}(\mathbf{z})$. If the result is equal to the message $\mathbf{d}$, the signature is accepted, otherwise rejected.

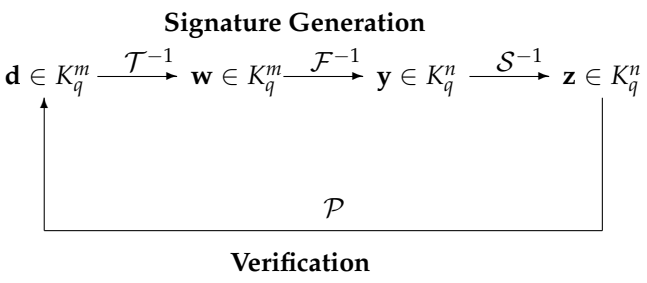

Figure 1. Two processes of multivariate signature schemes.

3.1. Unbalanced Oil and Vinegar Signature Scheme

Let $K = \mathbb{F}_q$ be the finite field with q elements, and let $n = v + o$ with v, o positive integers. An oil-vinegar quadratic polynomial over K is of the form:

$$\sum_{\substack{1\le i\le n\\ 1\le j\le v}} a_{ij}x_ix_j + \sum_{i=1}^{n} b_ix_i + c,$$

with coefficients $a_{ij}, b_i, c \in K$. The variables $x_1, \ldots, x_v$ are called vinegar variables and $x_{v+1}, \ldots, x_n$ the oil variables. Note that in an oil-vinegar polynomial, the oil and vinegar variables are not fully mixed, i.e., there are no quadratic terms x^2 for oil variables x. A UOV scheme is constructed as the following.

The central map $\mathcal{F} : K^n \to K^o, (x_1, \ldots, x_n) \mapsto (f^{(1)}, \ldots, f^{(o)})$ consists of o oil-vinegar polynomials:

$$f^{(1)} = \sum_{\substack{1\le i\le n\\ 1\le j\le v}} a_{ij}^{(1)}x_ix_j + \sum_{i=1}^{n} b_i^{(1)}x_i + c^{(1)},$$

$$\cdots\cdots\cdots$$

$$f^{(o)} = \sum_{\substack{1\le i\le n\\ 1\le j\le v}} a_{ij}^{(o)}x_ix_j + \sum_{i=1}^{n} b_i^{(o)}x_i + c^{(o)},$$

where the coefficients $a_{ij}^{(k)}, b_{ij}^{(k)}, c^{(k)}$ are in K. Choose randomly an invertible affine map $\mathcal{S} : K^n \to K^n$. The public key is given by $\mathcal{P} = \mathcal{F} \circ \mathcal{S} : K^n \to K^o$, and the private key consists of $\mathcal{F}$ and $\mathcal{S}$.

To sign a message $\mathbf{m} = (m_1, \ldots, m_o) \in K^o$, we do the following.

(1) Randomly choose vinegar values $a = (a_1, \ldots, a_v) \in K^v$, and plug them into the polynomials in the central map to obtain $\bar{f}^{(1)}, \ldots, \bar{f}^{(o)}$.
(2) Solving the linear system $\bar{f}^{(i)} = m_i$ with $i = 1, \ldots, o$ yields solution $(b_1, \ldots, b_o)$. If there is no solution, then go back to Step (1).
(3) Set $\mathbf{x} = (a_1, \ldots, a_v, b_1, \ldots, b_o)$. A signature is computed by $\mathbf{s} := \mathcal{S}^{-1}(\mathbf{x})$.
A signature $\mathbf{s}$ is accepted if $\mathcal{P}(\mathbf{s}) = \mathbf{m}$, otherwise it is rejected.

The public key of the scheme consists of o quadratic equations in n variables; hence, the public key has size:

$$o \cdot \frac{(n+1)(n+2)}{2} \quad \text{field elements}$$

and the size of the private key is:

$$n(n+1) + o \cdot \left(\frac{v(v+1)}{2} + v \cdot o + n + 1\right) \quad \text{field elements.}$$

3.2. Rainbow Signature Scheme

Rainbow signature schemes [13] are multi-layer versions of UOV schemes. For convenience, we introduce the two-layered Rainbow scheme (in the design, there is no advantage of using more than two layers). Let $K = \mathbb{F}_q$ be the finite field with q elements $n = v_1 + o_1 + o_2$ with v_1, o_1, o_2 positive integers. Set $m = o_1 + o_2$, $v_2 = o_1 + v_1$. The Rainbow central map $\mathcal{F} : K^n \to K^{o_1+o_2}, (x_1, \ldots, x_n) \mapsto (f_1, \ldots, f_{o_1+o_2})$ consists of the following $m = o_1 + o_2$ polynomials:

$$
\begin{aligned}
f^{(1)} &= \sum_{\substack{1\le i\le v_1+o_1\\ 1\le j\le v_1}} a_{ij}^{(1)} x_i x_j + \sum_{i=1}^{v_1+o_1} b_i^{(1)} x_i + c^{(1)},\\
&\cdots\cdots\cdots\\
f^{(o_1)} &= \sum_{\substack{1\le i\le v_1+o_1\\ 1\le j\le v_1}} a_{ij}^{(o_1)} x_i x_j + \sum_{i=1}^{v_1+o_1} b_i^{(o_1)} x_i + c^{(o_1)},\\
f^{(o_1+1)} &= \sum_{\substack{1\le i\le n\\ 1\le j\le v_1+o_1}} a_{ij}^{(o_1+1)} x_i x_j + \sum_{i=1}^{n} b_i^{(o_1+1)} x_i + c^{(o_1+1)},\\
&\cdots\cdots\cdots\\
f^{(o_1+o_2)} &= \sum_{\substack{1\le i\le n\\ 1\le j\le v_1+o_1}} a_{ij}^{(o_1+o_2)} x_i x_j + \sum_{i=1}^{n} b_i^{(o_1+o_2)} x_i + c^{(o_1+o_2)},
\end{aligned}
$$

where the coefficients $a_{ij}^{(k)}, b_{ij}^{(k)}, c^{(k)}$ are in K. Choose randomly two invertible affine maps $\mathcal{S} : K^n \to K^n$ and $\mathcal{T} : K^{o_1+o_2} \to K^{o_1+o_2}$. The public key is given by $\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S} : K^n \to K^{o_1+o_2}$, and the private key consists of $\mathcal{T}$, $\mathcal{F}$, and $\mathcal{S}$.

To sign a message $\mathbf{m} = (m_1, \ldots, m_{o_1+o_2}) \in K^{o_1+o_2}$, we first compute $\mathbf{y} = \mathcal{T}^{-1}(\mathbf{m}) = (y_1, \ldots, y_{o_1+o_2})$ and do the following.

(1) Choose $a = (a_1, \ldots, a_{v_1}) \in K^{v_1}$, and plug this into the polynomials in the central map to obtain $\bar{f}^{(1)}, \ldots, \bar{f}^{(o_1+o_2)}$.
(2) Solving the linear system $\bar{f}^{(i)} = y_i$ with $i = 1, \ldots, o_1$ yields solution $(b_1, \ldots, b_{o_1})$. If there is no solution, then go back to Step (1).
(3) Plug $(b_1, \ldots, b_{o_1})$ into $\bar{f}^{(o_1+1)}, \ldots, \bar{f}^{(o_1+o_2)}$, and solve the linear system $\bar{f}^{(i)} = y_i$ with $i = o_1 + 1, \ldots, o_1 + o_2$ to get a solution $(b_{o_1+1}, \ldots, b_{o_1+o_2})$. If there is no solution, then go back to Step (1).
(4) Set $\mathbf{x} = (a_1, \ldots, a_{v_1}, b_1, \ldots, b_{o_1+o_2})$. A signature is computed by $\mathbf{s} := \mathcal{S}^{-1}(\mathbf{x})$.

A signature $\mathbf{s}$ is accepted if $\mathcal{P}(\mathbf{s}) = \mathbf{m}$, otherwise it is rejected.

The public key of the scheme consists of m quadratic equations in n variables; hence, the public key has size:

$$m \cdot \frac{(n+1)(n+2)}{2} \quad \text{field elements}$$

and the size of the private key is:

$$m \cdot (m+1) + n(n+1) + \sum_{i=1}^{2} o_i \left(\frac{v_i(v_i+1)}{2} + v_i \cdot o_i + v_{i+1} + 1 \right) \quad \text{field elements,}$$

in which $v_3 := v_2 + o_2 = n$.

4. Modified UOV and Rainbow

4.1. Modified UOV Signature Scheme

The standard UOV scheme in Section 3.1 does not provide EUF-CMA security. Sakumoto et al. [17] modified the UOV scheme into a scheme that is EU-CMA secure. The difference with the standard UOV is the use of a binary salt r in the signature generation. The procedure is described as the following.

Key generation: With the input UOV parameters (q, v, o) and a length l of salt, generate the public key $\mathcal{P}$ and secret key $(\mathcal{F}, \mathcal{S})$ as in the standard Rainbow. Now, the public key and secret key of the modified Rainbow are $(\mathcal{P}, l)$ and $(\mathcal{F}, \mathcal{T}, \mathcal{S}, l)$, respectively.

Signature generation: To sign on a message $\mathbf{m}$, one does the following:

(1) Choose $a = (a_1, \ldots, a_{v_1}) \in K^v$.
(2) Choose a random salt $r \in \{0,1\}^l$.
(3) Let $\mathbf{h} = \mathcal{H}(\mathbf{m}\|r)$, where $\mathcal{H} : \{0,1\}^* \to K^o$ is a hash function.
(4) Solving the linear system $\bar{f}^{(i)} = h_i$ with $i = 1, \ldots, o$ yields solution $(b_1, \ldots, b_o)$. If there is no solution, then go back to Step (2).
(5) Set $\mathbf{x} = (a_1, \ldots, a_{v_1}, b_1, \ldots, b_o)$, and compute $\mathbf{s} := \mathcal{S}^{-1}(\mathbf{x})$. A signature is of the form $\sigma = (\mathbf{s}, r)$.

Verification: Given a message $\mathbf{m}$ and a signature $\sigma = (\mathbf{s}, r)$, one first computes $\mathbf{h} = \mathcal{H}(\mathbf{m}\|r)$ and $\mathbf{h}' = \mathcal{P}(\mathbf{s})$. If $\mathbf{h} = \mathbf{h}'$, then accept, otherwise reject.

It was proven in [17] that the modified UOV is EU-CMA secure if the underlying UOV scheme is secure, and it was mentioned that the modified UOV does not degrade the efficiency too much compared to the standard UOV; see [17] for more details.

4.2. Modified Rainbow Signature Scheme

The standard Rainbow scheme in Section 3.2 also does not provide EUF-CMA security. Here, we present a modified version that obtained EUF-CMA security, similar to [17] for UOV. The difference is the use of a random salt, which is a binary vector r. Instead of generating a signature for $\mathcal{H}(\mathbf{m})$, one generates a signature for $\mathcal{H}(\mathbf{m}\|r)$. The procedure is as follows.

Key generation: With input Rainbow parameters (q, v_1, o_1, o_2) and a length l of salt, generate the public key $\mathcal{P}$ and secret key $(\mathcal{F}, \mathcal{T}, \mathcal{S})$ as in the standard Rainbow. Now, the public key and secret key of the modified Rainbow are $(\mathcal{P}, l)$ and $(\mathcal{F}, \mathcal{T}, \mathcal{S}, l)$, respectively.

Signature generation: To sign on a message $\mathbf{m}$, one does the following:

(1) Choose $a = (a_1, \ldots, a_{v_1}) \in K^{v_1}$, and plug this into the polynomials in the central map to obtain $\bar{f}^{(1)}, \ldots, \bar{f}^{(o_1+o_2)}$ until the first o_1 linear polynomials $\bar{f}^{(1)}, \ldots, \bar{f}^{(o_1)}$ are non-degenerated, i.e., the corresponding coefficient matrix is invertible.
(2) Choose a random salt $r \in \{0,1\}^l$.
(3) Let $\mathbf{h} = \mathcal{H}(\mathbf{m}\|r)$.
(4) Compute $\mathbf{y} = \mathcal{T}^{-1}(\mathbf{h}) = (y_1, \ldots, y_{o_1+o_2})$.
(5) Solving the linear system $\bar{f}^{(i)} = y_i$ with $i = 1, \ldots, o_1$ yields solution $(b_1, \ldots, b_{o_1})$. This always has a solution since Step (1).
(6) Plug $(b_1, \ldots, b_{o_1})$ into $\bar{f}^{(o_1+1)}, \ldots, \bar{f}^{(o_1+o_2)}$, and solve the linear system $\bar{f}^{(i)} = y_i$ with $i = o_1 + 1, \ldots, o_1 + o_2$ to get a solution $(b_{o_1+1}, \ldots, b_{o_1+o_2})$. If there is no solution, then go back to Step (2).
(7) Set $\mathbf{x} = (a_1, \ldots, a_{v_1}, b_1, \ldots, b_{o_1+o_2})$, and compute $\mathbf{s} := \mathcal{S}^{-1}(\mathbf{x})$. A signature is of the form $\sigma = (\mathbf{s}, r)$.

Verification: Given a message $\mathbf{m}$ and a signature $\sigma = (\mathbf{s}, r)$, one first computes $\mathbf{h} = \mathcal{H}(\mathbf{m}\|r)$ and $\mathbf{h}' = \mathcal{P}(\mathbf{s})$. If $\mathbf{h} = \mathbf{h}'$ then accept, otherwise reject.

One easily proves the EU-CMA security of the modified Rainbow by following the same procedure as for the modified UOV scheme in [17].

4.3. Attacks

In this section, we review all currently-known (classical) attacks against Rainbow.

4.3.1. Direct Attacks

It is also well known that Rainbow schemes behave similarly to random systems, and therefore, we can estimate the complexity of direct attack against Rainbow as (cf. [20]):

$$\min_{k\geq 0} q^k \cdot \mathcal{O}\left(m \cdot \binom{n-k+d_{\text{reg}}-1}{d_{\text{reg}}}\right)^{\omega},$$

where $2 < \omega \leq 3$ is the linear algebra constant of solving a linear system and d_{reg} is the degree of regularity of the system, which can be estimated as the smallest d for which the coefficient of x^d in the expression:

$$\frac{(1-x^2)^m}{(1-x)^{m-k}}.$$

is non-positive.

4.3.2. The Rank Attacks

There are Minrank [21] and Highrank [22] attacks. The Minrank [21] attack tries to find a linear combination of the public key polynomials of minimal rank. In the case of Rainbow, such a minimal rank is v_2, which corresponds to a linear combination of polynomials in the first layer of the central map. The complexity is estimated as:

$$q^{v_1+1} \cdot m \cdot \left(\frac{n^3}{3} - \frac{m^2}{6}\right). \tag{1}$$

The Highrank [22] attack tries to identify variables that appear the lowest number of times in the polynomials of the central map. In the case of Rainbow, those are the oil variables of the last layer. The complexity of the Highrank attack is estimated as:

$$q^{o_2} \cdot \frac{n^3}{6}. \tag{2}$$

4.3.3. UOV Attack

One can consider Rainbow as a UOV scheme with $v = v_1 + o_1$ and $o = o_2$, and hence, it can be attacked by the UOV attack. Its goal is to find the pre-image of the oil subspace $\{x \in K^n : x_1 = \cdots = x_v = 0\}$ under the affine transformation $\mathcal{S}$. The complexity of this attack is estimated as:

$$q^{n-2o_2-1} \cdot o_2^4. \tag{3}$$

4.3.4. Rainbow-Band-Separation Attack

The Rainbow-Band-Separation (RBS) attack [23] tries to find linear transformations $\mathcal{S}$ and $\mathcal{T}$ that transform the public polynomials into ones of the form of polynomials in the central map of Rainbow, and hence find an equivalent key to forge a signature. To do this, one has to solve $m + n - 1$ equations in n variables. In our paper, we used the field $K = \mathbb{F}_{2^8}$, and we followed [20] to choose $n \geq \frac{5}{3}(m-1)$ so that the complexity of the RBS attack against Rainbow was at least the complexity of the direct attack.

4.3.5. Collision Attacks against the Hash Function

Note that the modified Rainbow scheme uses hash function $\mathcal{H} : \{0,1\}^* \to K^m$. Hence, in order to prevent a collision attack against the hash function, we need the number m of public equations satisfying that $m \cdot \log_2(q)$ is greater than the desired security level.

5. Identity-Based Signature Schemes Based on Rainbow

In this section, we follow the construction in Section 2 to instantiate an identity-based signature scheme based on the modified Rainbow scheme from Section 4.2. We call the scheme IBS-Rainbow.

5.1. Construction

Let q, v_1, o_1, o_2 be parameters as in Section 3.2. Let $K = \mathbb{F}_q$, $n = v + o_1 + o_2$, $m = o_1 + o_2$, and $v_2 = o_1 + v_1$. Let $\mathcal{H} : \{0,1\}^* \to K^m$ be a hash function and l be the length of salts. The scheme IBS-Rainbow consists of four algorithms $(\text{Setup}, \text{KeyDer}, \text{Sign}, \text{Vf})$ defined as follows.

Master-key generation: $(mpk, msk) \leftarrow \text{Setup}(1^k)$.

The algorithm Setup selects a central map $\mathcal{F} : K^n \to K^m$ for a Rainbow scheme with parameters as above, two invertible affine maps $\mathcal{S} : K^n \to K^n$, $\mathcal{T} : K^m \to K^m$, and computes $\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S} : K^n \to K^m$. It outputs the master secret key $msk \leftarrow (\mathcal{F}, \mathcal{S}, \mathcal{T})$ and the master public key $mpk \leftarrow \mathcal{P}$.

User-key extraction: $usk_I \leftarrow \text{KeyDer}(msk, I)$.

For a user I, the algorithm KeyDer generates a new Rainbow scheme with secret key $sk_I \leftarrow (\mathcal{F}_I, \mathcal{S}_I, \mathcal{T}_I)$ and public key $pk_I \leftarrow \mathcal{P}_I = \mathcal{T}_I \circ \mathcal{F}_I \circ \mathcal{S}_I$ such that $(\mathcal{F}_I, \mathcal{S}_I, \mathcal{T}_I)$ is different from the master secret key $(\mathcal{F}, \mathcal{S}, \mathcal{T})$. Then, it executes $d_I \leftarrow \mathcal{H}(\mathcal{P}_I \| I)$. Next, it uses the knowledge of master secret key $msk \leftarrow (\mathcal{F}, \mathcal{S}, \mathcal{T})$ to find a signature (σ_{cI}, r_{cI}) for the message d_I as in Section 4.2. Note that $\mathcal{P}(\sigma_{cI}) = \mathcal{H}(d_I \| r_{cI})$. Let $cert_I \leftarrow (\sigma_{cI}, r_{cI})$. The algorithm then returns the secret key for the user I as $usk_I \leftarrow (sk_I, pk_I, cert_I)$.

Signature generation: $\sigma \leftarrow \text{Sign}(usk_I, M)$.

Given a message M, the algorithm uses the knowledge of usk_I to find a signature (σ_I, r_I) for M from the system $\mathcal{P}_I = \mathcal{T}_I \circ \mathcal{F}_I \circ \mathcal{S}_I$ as in Section 4.2. It outputs the signature $\sigma \leftarrow (pk_I, cert_I, (\sigma_I, r_I))$.

Verification: $\{0,1\} \leftarrow \text{Vf}(mpk, I, M, \sigma)$.

Given a signature σ of a message M of the user I. Parse σ as $(pk_I, cert_I, (\sigma_I, r_I))$. Note that $mpk \leftarrow \mathcal{P}$, $pk_I \leftarrow \mathcal{P}_I$ and $cert_I \leftarrow (\sigma_{cI}, r_{cI})$. We then compute $\mathbf{h} = \mathcal{P}(\sigma_{cI})$, $\mathbf{h}' = \mathcal{P}_I(\sigma_I)$. If both $\mathbf{h} = \mathcal{H}(\mathcal{H}(\mathcal{P}_I \| I), r_{cI})$ and $\mathbf{h}' = \mathcal{H}(M \| r_I)$, then it outputs one, which means the signature is accepted. Otherwise, it outputs zero and rejects the signature.

The correctness is easy to check. Since we are using the modified Rainbow scheme in Section 4.2, which is EU-CMA secure, the resulting IBS-Rainbow scheme is also EU-CMA secure.

5.2. Parameters

We next give a choice of parameters and compute the key sizes of the IBS-Rainbow. We also revised the IBUOV scheme in [16] (note that the construction of the IBUOV scheme also follows the same route as in Section 5.1 with the core modified Rainbow (Section 4.2) replaced by the normal UOV scheme (the scheme in Section 4.1 without using salts and the hash function in Steps (2) and (3) of the signature generation process); see Appendix A for more details.) and compared it with IBS-Rainbow.

First, for the EU-CMA security of the system, we needed to ensure that no salt was used for more than one signature. Under the assumption of up to 2^{64} signatures being generated with the system, we chose the length l of the salt to be $l = 128$ bit, independent of the security level.

Second, we chose two popular base fields for K, which were $\mathbb{F}_{2^8}$ and $\mathbb{F}_{31}$. We aimed for the security level to be the standard 128-bit. The choice of parameters had to ensure that the corresponding Rainbow scheme was secure against all attacks mentioned in Section 4.3, i.e., for a choice of parameters, the complexities of all attacks in Section 4.3 had to be at least 2^k for corresponding security level k ($k = 128$).

The details are illustrated in Table 1. We write IBUOV(q, o, v), meaning that (q, o, v) is the parameter of the UOV scheme used in IBUOV. Similarly, we write IBS-Rainbow(q, v_1, o_1, o_2) with (q, v_1, o_1, o_2) the parameter of the Rainbow scheme used in IBS-Rainbow.

Table 1. Comparison of key sizes and signature lengths at the 128-bit security level.

Security Level (bit)	Scheme Parameters	Hash Length (bit)	User's Signature Size (KB)	mpk Size (KB)	msk Size (KB)	usk Size (KB)
128	IBUOV$(2^8, 90, 45)$	360	714.4	409.4	381.8	942.2
	IBS-Rainbow$(2^8, 40, 24, 24)$	384	395.7	187.7	140.0	431.7
	IBUOV$(31, 104, 52)$	256	659.9	419.9	389.2	929.1
	IBS-Rainbow$(31, 36, 28, 28)$	268	304.3	148.3	103.7	330

As we see from Table 1, using Rainbow, we can reduce the key sizes and signature sizes. In particular, we reduced the signature sizes up to 50%. For the user's secret key size, we can reduce up to 55% and 65% for the fields $\mathbb{F}_{2^8}$ and $\mathbb{F}_{31}$, respectively.

6. Conclusions

In this paper, we instantiated an identity-based signature scheme based on a provably-secure Rainbow signature scheme, IBS-Rainbow. We also revisited the previous identity-based signature scheme IBUOV based on UOV [16] and noted that IBUOV is not EU-CMA secure since the underlying UOV scheme is not EU-CMA secure, and the proposed security parameters and key sizes of IBUOV are not correct. We revised again and compared it with our IBS-Rainbow. As a result, IBS-Rainbow was much more efficient than IBUOV in terms of key sizes and signature sizes. There are possibilities to optimize the key sizes by applying the methods in [24–26]. We will leave it as a future work for further optimization, both in terms of key sizes and security under the quantum random oracle model.

Funding: The research is funded by by Vietnam National University Ho Chi Minh City (VNU-HCM) under grant number C2017-18-03.

Acknowledgments: The author would like to thank Dung H. Duong and Ha Tran for useful discussions.

Conflicts of Interest: The author declares no conflict of interest.

Appendix A. The Construction of IBUOV

We recall the construction of IBUOV [16] for completeness. In the original construction [16], the authors used the original UOV scheme in Section 3.1. However, as mentioned above, that UOV scheme is not EU-CMA secure, and hence, the resulting IBUOV is not EU-CMA secure. We modified IBUOV by using the modified UOV scheme in Section 4.1 and the parameters (in Table 1) accordingly. The construction of IBUOV is as follows.

Let q, v, o be parameters as in Section 3.1. Let $K = \mathbb{F}_q$, $n = v + o$, and $m = o$. Let $\mathcal{H} : \{0,1\}^* \to K^m$ be a hash function. The scheme IBUOV consists of four algorithms $(\text{Setup}, \text{KeyDer}, \text{Sign}, \text{Vf})$ defined as the following.

Master-key generation: $(mpk, msk) \leftarrow \text{Setup}(1^k)$.

The algorithm Setup selects a central map $\mathcal{F} : K^n \to K^m$ for a Rainbow scheme with parameters as above, an invertible affine map $\mathcal{S} : K^n \to K^n$, and computes $\mathcal{P} = \mathcal{F} \circ \mathcal{S} : K^n \to K^m$. It outputs the master secret key $msk \leftarrow (\mathcal{F}, \mathcal{S})$ and the master public key $mpk \leftarrow \mathcal{P}$.

User-key extraction: $usk_I \leftarrow \text{KeyDer}(msk, I)$.

For a user I, the algorithm KeyDer generates a new Rainbow scheme with secret key $sk_I \leftarrow (\mathcal{F}_I, \mathcal{S}_I)$ and public key $pk_I \leftarrow \mathcal{P}_I = \mathcal{F}_I \circ \mathcal{S}_I$ such that $(\mathcal{F}_I, \mathcal{S}_I)$ is different from the master secret key $(\mathcal{F}, \mathcal{S})$. Then, it executes $d_I \leftarrow \mathcal{H}(\mathcal{P}_I \| I)$. Next, it uses the knowledge of master secret key $msk \leftarrow (\mathcal{F}, \mathcal{S})$

to find a signature (σ_{cI}, r_{cI}) for the message d_I as in Section 4.2. Note that $\mathcal{P}(\sigma_{cI}) = \mathcal{H}(d_I \| r_{cI})$. Let $cert_I \leftarrow (\sigma_{cI}, r_{cI})$. The algorithm then returns the secret key for the user I as $usk_I \leftarrow (sk_I, pk_I, cert_I)$.

Signature generation: $\sigma \leftarrow \text{Sign}(usk_I, M)$.

Given a message M, the algorithm uses the knowledge of usk_I to find a signature (σ_I, r_I) for M from the system $\mathcal{P}_I = \mathcal{F}_I \circ \mathcal{S}_I$ as in Section 4.2. It outputs the signature $\sigma \leftarrow (pk_I, cert_I, (\sigma_I, r_I))$.

Verification: $\{0, 1\} \leftarrow \text{Vf}(mpk, I, M, \sigma)$.

Given a signature σ of a message M of the user I. Parse σ as $(pk_I, cert_I, (\sigma_I, r_I))$. Note that $mpk \leftarrow \mathcal{P}$, $pk_I \leftarrow \mathcal{P}_I$, and $cert_I \leftarrow (\sigma_{cI}, r_{cI})$. We then compute $\mathbf{h} = \mathcal{P}(\sigma_{cI})$, $\mathbf{h}' = \mathcal{P}_I(\sigma_I)$. If both $\mathbf{h} = \mathcal{H}(\mathcal{H}(\mathcal{P}_I \| I), r_{cI})$ and $\mathbf{h}' = \mathcal{H}(M \| r_I)$, then it outputs one, which means the signature is accepted. Otherwise, it outputs zero and rejects the signature.

References

1. Shor, P. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. Comput.* **1997**, *26*, 1484–1509. [CrossRef]
2. Rivest, R.L.; Shamir, A.; Adleman, L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
3. Kravitz, D. Digital Signature Algorithm. U.S. Patent 5,231,668, 27 July 1993.
4. Koblitz, N. Elliptic curve cryptosystems. *Math. Comp.* **1987**, *48*, 203–209. [CrossRef]
5. National Institute of Standards and Technology: Report on Post Quantum Cryptography. NISTIR Draft 8105. Available online: https://csrc.nist.gov/publications/detail/nistir/8105/final (accessed on 17 March 2019).
6. National Institute of Standards and Technology: Post-Quantum Cryptography—Round 1 Submission. Available online: https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions (accessed on 17 March 2019).
7. National Institute of Standards and Technology: First PQC Standardization Conference. Available online: https://csrc.nist.gov/events/2018/first-pqc-standardization-conference (accessed on 17 March 2019).
8. Chen, A.I.T.; Chen, M.-S.; Chen, T.-R.; Cheng, C.-M.; Ding, J.; Kuo, E.L.-H.; Lee, F.Y.-S.; Yang, B.-Y. SSE implementation of multivariate PKCs on modern x86 cpus. In Proceedings of the Cryptographic Hardware and Embedded Systems—CHES 2009, Lausanne, Switzerland, 6–9 September 2009; Volume 5747, pp. 33–48.
9. Bogdanov, A.; Eisenbarth, T.; Rupp, A.; Wolf, C. Time-area optimized public-key engines: MQ-cryptosystems as replacement for elliptic curves? In Proceedings of the Cryptographic Hardware and Embedded Systems—CHES 2008, Washington, DC, USA, 10–13 August 2008; Volume 5154, pp. 45–61.
10. Matsumoto, T.; Imai, H. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques, Davos, Switzerland, 25–27 May 1988; Volume 330, pp. 419-453.
11. Patarin, J. Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt 88. In Proceedings of the 15th Annual International Cryptology Conference, Santa Barbara, CA, USA, 27–31 August 1995; Volume 963, pp. 248–261.
12. Kipnis, A.; Patarin, L.; Goubin, L. Unbalanced Oil and Vinegar Schemes. In Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, 2–6 May 1999; Volume 1592, pp. 206–222.
13. Ding, J.; Schmidt, D.S. Rainbow, a new multivariate polynomial signature scheme. In Proceedings of the Applied Cryptography and Network Security, ACNS 2005, New York, NY, USA, 7–10 June 2005; Volume 3531, pp. 164–175.
14. Shamir, A. Identity-based cryptosystems and signature schemes. In Proceedings of the CRYPTO 1984, Santa Barbara, CA, USA, 19–22 August 1984; pp. 19–23.
15. Boneh, D.; Franklin, M.K. Identity based encryption from the Weil pairing. *SIAM J. Comput.* **2003**, *32*, 586–615. [CrossRef]

16. Shen, W.; Tang, S.; Xu, L. IBUOV, A Provably Secure Identity-Based UOV Signature Scheme. In Proceedings of the 2013 IEEE 16th International Conference on Computational Science and Engineering, CSE 2013, Sydney, Australia, 3–5 December 2013; pp. 388–395.
17. Sakumoto, K.; Shirai, T.; Hiwatari, H. On provable security of UOV and HFE signature schemes against chosen-message attack. In Proceedings of the 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, 29 November–2 December 2011; Volume 7071, pp. 68–82.
18. Kiltz, E.; Neven, G. Identity-based Signatures. In *Identity-Based Cryptography*; Joye, M., Neven, G., Eds.; Volume 2 of Cryptology and Information Security Series; IOS Press: Amsterdam, The Netherlands, 2008; pp. 31–44.
19. Garey, M.R.; Johnson, D.S. *Computers and Intractability: A Guide to the Theory of NP-Completeness*; W.H. Freeman and Company: New York, NY, USA, 1979.
20. Petzoldt, A.; Bulygin, S.; Buchmann, J.A. Selecting Parameters for the Rainbow Signature Scheme. In Proceedings of the Third International Workshop, PQCrypto 2010, Darmstadt, Germany, 25–28 May 2010; Volume 6061, pp. 218–240.
21. Billet, O.; Gilbert, H. Cryptanalysis of Rainbow. In Proceedings of the 5th International Conference, SCN 2006, Maiori, Italy, 6–8 September 2006; Volume 4116, pp. 336–347.
22. Coppersmith, D.; Stern, J.; Vaudenay, S. Attacks on the birational permutation signature schemes. In Proceedings of the Advances in Cryptology—CRYPTO' 93, Santa Barbara, CA, USA, 22–26 August 1993; Volume 773, pp. 435–443.
23. Ding, J.; Yang, B.Y.; Chen, C.H.O.; Chen, M.S.; Cheng, C.M. New Differential-Algebraic attacks and Reparametrization of Rainbow. In Proceedings of the Applied Cryptography and Network Security, ACNS 2008, New York, NY, USA, 3–6 June 2008; Volume 5037, pp. 242–257.
24. Petzoldt, A.; Bulygin, S.; Buchmann, J. CyclicRainbow—A multivariate signature scheme with a partially cyclic public key. In Proceedings of the 11th International Conference on Cryptology, Hyderabad, India, 12–15 December 2010; Volume 6498, pp. 33–48.
25. Duong, D.H.; Van Luyen, L.; Tran, H. Choosing subfields for LUOV and LRainbow Signature Scheme. Unpublished work, 2018.
26. Beullens, W.; Preneel, B. Field Lifting for Smaller UOV Public Keys. In Proceedings of the 18th International Conference on Cryptology, Chennai, India, 10–13 December 2017; Volume 10698, pp. 227–246.