Mathematical Biosciences and Engineering

MBE, 16(6): 7734–7750.
DOI: 10.3934/mbe.2019388
Received: 16 June 2019
Accepted: 18 August 2019
Published: 23 August 2019

http://www.aimspress.com/journal/MBE

Research article

An improved signature model of multivariate polynomial public key cryptosystem against key recovery attack

Xin Wang[1,2] and Bo Yang[1,*]

[1] School of Computer Science, Shaanxi Normal University, Xi'an, 710119, China
[2] School of Electronic Information and Artificial Intelligence, Shaanxi University of Science & Technology, Xi'an, 710021, China

*** Correspondence:** Email: byang@snnu.edu.cn; Tel: ++00862986168633.

Abstract: An improved signature model of multivariate polynomial public key cryptosystem to resist the key recovery attack is presented in this paper. Two pairs of public keys are added to design new authentication conditionals for public keys, and then the verification is not only to verify the original external information but also the exact internal kernel information. It requires both the corresponding private key and the exact internal node information to produce an accurate signature, so that a forged signature by key recovery attack cannot pass the verification without the exact private key. To illustrate this, the classic HFE (Hidden Fields Equations) scheme is taken as an example to clarify the signing and verifying process in detail. It provides a useful supplement to the research and designing of secure digital signature schemes in the quantum age.

Keywords: multivariate polynomial; public key cryptosystem; signature; key recovery attack

1. Introduction

Post-quantum cryptosystem has grown about 30 years. Especially in the past 10 years, the field of signature developed in leaps and bounds and emerged many research. Hash-based signature schemes are still the most promising cryptosystem candidates in a post-quantum world, such as eXtended Merkle Signature Scheme (XMSS) [1] and G-Merkle [2] XMSS, which only rely on the properties of cryptographic hash functions instead of the conjectured hardness of mathematical problems. XMSS provides strong security guarantees and is even secure when the collision resistance of the underlying hash function is broken. Hash-based signatures can so far withstand

known attacks using quantum computers. And another kind new research is Hysteresis Digital Signature for keyed hash chain with one-time signatures. The hysteresis signature calculates the hash value for the data generated only at that point and the short data, such as the hash value of the data at the previous point. Hysteresis signatures [3,4] have a linking structure is constructed between the signatures. It is applicable to verify the non-alteration of total data for maintaining the long-term reliability and relevance of digital signatures. For example, the file server manager and the auditor can verify the hysteresis signature chain sequentially from the most recent one to the oldest one. In other words, the integrity of each file can be verified with the hysteresis signature scheme, which makes it impossible to implement rollback and reordering attacks. So the mechanism is different in our scheme of multivariate public key cryptosystem. In hysteresis signatures, it is difficult to make falsification of a file, because it would mandate the reconstruction of the linked structure of all newer signatures in order to remain undetected. However, in multivariate public key cryptosystem, the equivalent keys always exist. So a falsification signature generated by equivalent key can always be generated and it can certainly pass the verification. So our purpose is to reduce the potential threats caused by rank attack of equivalent key of multivariate public key cryptosystem itself.

The multivariable public key cryptosystem, which differs from two traditional public key cryptosystems RSA or ECC, is another kind of post-quantum cryptosystem [5,6] and has aroused much attention in recent years. It is designed with a set of nonlinear multivariable equations on finite field. Its security is based on the fact that solving a set of multivariable quadratic polynomial equations is a NP-C problem, which is called MQ-problem (multivariate quadratic problem) [7]. On January 30, 2019, NIST (National Institute of Standards and Technology) launched a global solicitation campaign of post-quantum public key cryptography standard draft. After one year of proposal collection and first round review, 26 algorithms were selected from the initial 69 and entered the semi-finals of post-quantum cryptography. In this candidate algorithm, there are 9 signatures algorithms .and Among these signatures algorithms, 4 signatures LUOV, Rainbow [8,9], MQDSS [10] and GeMSS are based on multivariate polynomials, This multivariate public key cryptography shows great potential. Especially, the MQDSS signature scheme is designed from a new construction idea based on the multivariate identity authentication protocol [10]. Along the way, different multivariate signature schemes with special signature characteristics have emerged in recent years, such as blind signatures [11]. These schemes are different from the previously designed multivariate digital signature schemes, which are all based on the underlying security authentication protocol and the security, can be directly reduced to the MQ problem.

The key recovery attack for multivariate polynomial public key cryptosystem [12], since there are superfluous equivalent keys in its key space [13,14], is an effective method to analyze multivariate cryptosystems. However, the original signature model of multivariable system did not take the potential threat such as the key recovery attack into account. Then most of the existing encryption or signature schemes are vulnerable to key recovery attack [15–19]. In those schemes, only the message and the signature themselves are taken into account when designing a signature scheme in the original model. Those schemes do not involve the internal information in verifying process as the cause that they are crashed easily. In fact, people cannot verify that how the signature comes from through the original signature model. The forged signature is likely to produce by some equivalent key [20]. Because the signature is generated whether by the exact private key or the equivalent private key are corresponding to the same public key. As indicated in [21], the author describe a key recovery attack for ZHFE (A scheme utilizes as core map two HFE polynomials and

the basic idea for the construction comes from the Zhuang-Zi algorithm [22]) using the MinRank approach shows that such linear combinations can be efficiently extracted from the public key and then linear combinations can be efficiently extracted from the public key. Although in some research [23], the authors claim that their scheme is secure against direct and Rank attacks of the Kipnis-Shamir/Bettale type, however there still have some reservations. The situation is only temporary，because the existence of equivalent keys in multivariate public key cryptosystem induces a structural weakness [24]. This point of view is also reflected in [25]. So we have reason to think the weakness the inherent characteristic of classic multivariate public key cryptosystem signature model.

The idea of key recovery attack is to find another private key and not knowing the exact valid private key of one same public key. This is the fact that multivariate public key cryptosystem has a large number of equivalent redundant keys [13,14]. Therefore, the attacker can use the equivalent private key of the public key to forge a signature without knowing the real private key, and this signature followed from the equivalent private key can also be verified by the public key. Therefore, the forged signature is produced successfully. In this paper, by adding two pairs of public keys and corresponding verification of the crucial internal node information, we propose an improved multivariate signature model resisting the key recovery attack. In this paper we aim to resist the key recovery attack by adding auxiliary information in the verification when the signature is generated. To eliminate all possibility that the signature generated by the equivalent key, which also passes the verification, the additional public key is used to verify its internal node information. So that, the signature can only be generated by the user who has the real legal key and the threat of the key recovery attack can be resisted. The model is generic construction and applicable for existing multivariate scheme's construction, In this paper, we take the classic HFE (Hidden Fields Equations) scheme HFE [26] as an example to illustrate that the advantages of the improved model is more secure than the original model at the expense of taking a little more time. Moreover, the design of the improved signature model is universal and it can be widely applied in existing multivariate schemes.

The security targets and adversary model of key recovery attack is different from the chosen-message attacks (EUF-CMA) of a signature scheme. EUF-CMA is to prove existentially unforgeable under chosen message attack for a concrete scheme. The key recovery attack here is only to the universal model of the multivariate polynomial public key system and it is a more fundamental issue than the EUF-CMA security of a concrete scheme. The adversary model is he has only the ability of obtaining the equivalent key from the public key and the security aim is to build a universal construction of multivariate signature model which resists the key recovery attack. Because, Wolf [13,14] observed a fact that multiple private keys correspond to one public key is an essential characteristic of multivariate public key system, and up to now, most existing multivariable signature schemes generated by the universal model are often vulnerable to key recovery attack. So we propose an improved multivariate signature model resisting the key recovery attack by adding two pairs of public keys and corresponding verification of the crucial internal node information. Thus this paper mainly analyzes the security and performance of the multivariable universal signature structure in the key recovery attack.

As for the public key certificate, we give a briefly introduction. Google with block chain is to document valid certificates is a new study and it has good research prospects. While based on the published research, Public Key Infrastructure (PKI) is used to solve the man-in-the-middle attack with certificates that authenticate the transmitted public key in multivariate polynomials public key cryptosystem is the same as that in classic public key cryptosystem. The certificate itself is a linked

list of public keys and signatures, where each signature authenticates the next public key under the previous one. The first public key in this link is the root public key of a Certificate Authority, which in the case of web traffic is built into the user's browser [27]. And the transmission of the certificate constitutes a significant bandwidth cost in any key establishment protocol and should consequently be minimized. In [28], the author explains how to transform any MQ signature scheme into one with a much smaller public key at the cost of a larger signature.

The paper is organized as follows. The preliminaries are briefly described in Section 1. The original signature model of multivariate polynomial cryptosystem is showed in Section 2. Section 3 introduces the improved signature model of multivariate cryptosystem. The comparison of our proposed scheme with the original model is discussed in Section 4. Finally, we conclude this paper in Section 5.

2. The original signature model of multivariable public key cryptosystem

F is a finite field. $(\mathcal{T},\mathcal{Q},\mathcal{S})$ is the trapdoor information. $\mathcal{S}$ and $\mathcal{T}$ are randomly selected reversible affine transformations in F^n and F^m, where $\mathcal{S}:\boldsymbol{u}\to\boldsymbol{x}=\boldsymbol{M}_S\boldsymbol{u}+\boldsymbol{c}_S\in \mathrm{Aff}^{-1}\left(\mathrm{F}^n\right)$, and $\mathcal{T}:\boldsymbol{y}\to\boldsymbol{v}=\boldsymbol{M}_{\mathcal{T}}\boldsymbol{y}+\boldsymbol{c}_{\mathcal{T}}\in \mathrm{Aff}^{-1}\left(\mathrm{F}^m\right)$. $\mathcal{Q}$ is a central mapping. It is usually made up of m quadratic polynomial equations of n variables:

$$\mathcal{Q}\left(x_1,\mathrm{L}\ ,x_n\right)\mathrm{a}\ \left(q_1\left(x_1,\mathrm{L}\ ,x_n\right),\mathrm{L}\ ,q_m\left(x_1,\mathrm{L}\ ,x_n\right)\right).$$

The structure is usually open or partially confidential. $\mathcal{S}$ and $\mathcal{T}$ "hide" the center mapping equation $\mathcal{Q}$. Triple $(\mathcal{T},\mathcal{Q},\mathcal{S})$ is usually as a private key and the corresponding public key is $\mathcal{P}\left(x_1,\mathrm{L}\ ,x_n\right)=\mathcal{T}\,\mathrm{o}\mathcal{Q}\,\mathrm{o}\mathcal{S}\left(x_1,\mathrm{L}\ ,x_n\right)=\left(p_1\left(x_1,\mathrm{L}\ ,x_n\right),\mathrm{L}\ ,p_m\left(x_1,\mathrm{L}\ ,x_n\right)\right)$.

Public Key: $\mathcal{P}$.

Private Key: $\mathcal{Q},\mathcal{S},\mathcal{T}$.

The original model of the signature and verification of multivariate public key cryptosystem [29,30] is given as Figure 1.

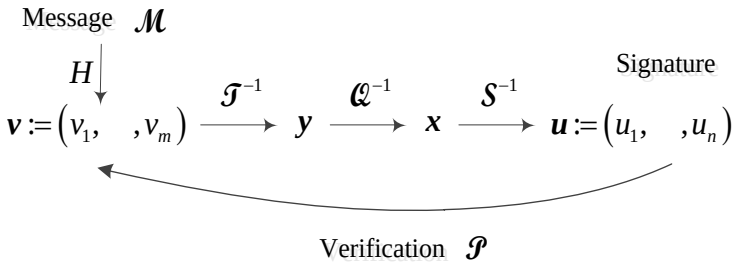

Figure 1. The original signature model of multivariate public key cryptosystem.

2.1. Signature generation

$\mathcal{M}$ is a message. Taking a hash function H, we have $\boldsymbol{v} = H(\mathcal{M})$. Then $\boldsymbol{y} = \mathcal{T}^{-1}(\boldsymbol{v})$, $\boldsymbol{x} = \mathcal{Q}^{-1}(\boldsymbol{y})$ and $\boldsymbol{u} = \mathcal{S}^{-1}(\boldsymbol{x})$ are calculated in turn, where $\mathcal{S}^{-1}$, $\mathcal{T}^{-1}$ and $\mathcal{Q}^{-1}$ are reversible affine transformations of private key $\mathcal{S}$, $\mathcal{T}$ and the central mapping $\mathcal{Q}$ respectively. Vector $\boldsymbol{u} = (u_1, \mathrm{L}\ , u_n)$ is the signature of message $\mathcal{M}$.

2.2. Verification

A signature $\boldsymbol{u}$ is accepted if $\boldsymbol{v} = \mathcal{P}(\boldsymbol{u})$ using the public key $\mathcal{P}$. As shown in Figure 1, a signature $\boldsymbol{u}$ is accepted if $\boldsymbol{v} = \mathcal{P}(\boldsymbol{u})$ using the public key $\mathcal{P}$. We call the signature $\boldsymbol{u}$ is passed the public key verification and the signature $\boldsymbol{u}$ is a valid signature.

2.3. Key recovery attack

Definition 1 Equivalent private keys [13,14]: For a cryptosystem, if two (or more) private keys

$$(\mathcal{T}_1, \mathcal{Q}_1, \mathcal{S}_1) \text{ and } (\mathcal{T}_2, \mathcal{Q}_2, \mathcal{S}_2) \in \mathrm{Aff}^{-1}(\mathrm{F}^m) \times \mathrm{MQ}(\mathrm{F}^n, \mathrm{F}^m) \times \mathrm{Aff}^{-1}(\mathrm{F}^n)$$

correspond to the same public key, we call the two (multiple) private keys "equivalent", which have: $\mathcal{T}_1 \mathrm{o} \mathcal{Q}_1 \mathrm{o} \mathcal{S}_1 = \mathcal{P} = \mathcal{T}_2 \mathrm{o} \mathcal{Q}_2 \mathrm{o} \mathcal{S}_2$. For example, $(\mathcal{T}', \mathcal{Q}', \mathcal{S}')$ is an equivalent key of the private key $(\mathcal{T}, \mathcal{Q}, \mathcal{S})$, then according Definition 1, we have $\mathcal{T} \mathrm{o} \mathcal{Q} \mathrm{o} \mathcal{S} = \mathcal{P} = \mathcal{T}' \mathrm{o} \mathcal{Q}' \mathrm{o} \mathcal{S}'$. Then for a message $\boldsymbol{v}$, we get the correct and valid signature $\boldsymbol{u} = \mathcal{T}^{-1} \mathrm{o} \mathcal{Q}^{-1} \mathrm{o} \mathcal{S}^{-1}(\boldsymbol{v})$ by using the private key $(\mathcal{T}, \mathcal{Q}, \mathcal{S})$. And there is also $\boldsymbol{u}' = \mathcal{T}' \mathrm{o} \mathcal{Q}' \mathrm{o} \mathcal{S}'(\boldsymbol{v})$ by using the equivalent key $(\mathcal{T}', \mathcal{Q}', \mathcal{S}')$. Be notice that according Definition 1, there is $\boldsymbol{v} = \mathcal{P}(\boldsymbol{u}) = \mathcal{P}(\boldsymbol{u}')$. That is to say for the fake signature $\boldsymbol{u}'$, there is $\boldsymbol{u}' \neq \boldsymbol{u}$ and $\boldsymbol{u}'$ can pass the verification.

Definition 2 Key recovery attack: A public key $\mathcal{P}$ is known. This type of attack is to find more intrinsic links between the variables of the public key and to generate more multivariable public key equations which are independent of the original equations, then to solve the equivalent keys from the public key.

In other words, the key recovery attack depends on linear algebra in all kinds of spaces of homogeneous polynomials [31]. When the attacker finds a decomposition of public key $\mathcal{P}$, that is to say he find the equivalent key $\mathcal{T}_2$, $\mathcal{S}_2$ (and $\mathcal{Q}_2$), and it is very easy to forge a signature in the scheme. For example, the Unbalanced Oil and Vinegar Scheme (UOV) ~~has~~ have such an equivalent key with

probability roughly [32]. Besides, in some sense, the key recovery attack coincides with the EIP-problem (Extended Isomorphism of Polynomials[1]) [33]. And the EIP-problem of Matrix-based UOV can be solved in polynomial-time in [34], and then the Matrix-based UOV signature can be forged at appropriate parameters at 80 or 100 security levels. Therefore, key-recovery attack helps find an equivalent key and fork signature by using algebraic structure of concrete trapdoor of scheme.

3. Improved signature model of multivariable public key cryptosystem

The original signature model is described as Figure 1 in Section 1, and we also hash the message before we make the signature. This is for compression only as in tradition public key cryptosystem. We use secret hash function to generate the public key in the improved model, then we would like to stress that this is only to hide the private key as hash function is irreversible and anti-collision. And we will regard the hash as a random oracle. Moreover, as we know the known quantum decomposition algorithm has no advantage in such as SHA-3.

3.1. Generating system parameters

Similarly, let F be a finite field and E be a n-th power extension field of F, n-th and m-th extension fields of F are denoted as F^n and F^m respectively. The isomorphic mapping $\pi:\mathrm{E}\to\mathrm{F}^n$ is defined from the extended domain to vector space. Take a central mapping $\mathcal{Q}$, two reversible affine transformations $\mathcal{S}$ and $\mathcal{T}$.

Then randomly select a set of n variable quadratic multivariable polynomial equation vector $\left(g_1\left(x_1,\mathrm{L}\ ,x_n\right),\mathrm{L}\ ,g_n\left(x_1,\mathrm{L}\ ,x_n\right)\right)$, which denoted as $\mathcal{G}$, $\mathcal{G}(\boldsymbol{x})=\left(g_1(\boldsymbol{x}),\mathrm{L}\ ,g_n(\boldsymbol{x})\right)$, and two one-way irreversible polynomials $\mathcal{H}$ and $\mathcal{H}'$ on F^n. The user's private key consists of $\mathcal{Q}$, $\mathcal{S}$, $\mathcal{T}$ and $\mathcal{G}$, all of which are invertible affine transformations. $\mathcal{H}$ and $\mathcal{H}'$ are secretly selected for public key generation. The public key is composed of five parts: $\mathcal{P}=\mathcal{T}\circ\mathcal{Q}\circ\mathcal{S}$, $\mathcal{H}\circ\mathcal{G}^{-1}\circ\mathcal{S}$, $\mathcal{H}\circ\mathcal{S}$, $\mathcal{H}'\circ\mathcal{Q}\circ\mathcal{G}^{-1}\circ\mathcal{S}$, and $\mathcal{H}'\circ\mathcal{T}^{-1}$. The signature generation progress and signature verification progress are as shown in Figure 2.

Public Key: F, $\mathcal{P}$, $\mathcal{H}\circ\mathcal{G}^{-1}\circ\mathcal{S}$, $\mathcal{H}\circ\mathcal{S}$, $\mathcal{H}'\circ\mathcal{Q}\circ\mathcal{G}^{-1}\circ\mathcal{S}$, $\mathcal{H}'\circ\mathcal{T}^{-1}$.

Private Key: $\mathcal{Q},\mathcal{G},\mathcal{S},\mathcal{T}$.

[1] EIP-problem: Let public key $\mathcal{P}$ be nonlinear multivariate systems $\mathcal{P}=\mathcal{T}_1\circ\mathcal{Q}_1\circ\mathcal{S}_1$ with a linear maps, and $\mathcal{S}_1$, $\mathcal{T}_1$ and trapdoor $\mathcal{Q}_1$ belongs to some special class of multivariate polynomial systems, find another decomposition of $\mathcal{P}$ such that $\mathcal{P}=\mathcal{T}_2\circ\mathcal{Q}_2\circ\mathcal{S}_2$ with a linear maps $\mathcal{S}_2$, $\mathcal{T}_2$ and $\mathcal{Q}_2$.

3.2. The signature generation

(1) For message $\boldsymbol{u}$, the signer uses secret key $\mathcal{T}$ to calculate $(y_1,\mathrm{L}\ ,y_m)=\mathcal{T}^{-1}(u_1,\mathrm{L}\ ,u_m)$ and denotes $(y_1,\mathrm{L}\ ,y_m)$ as $\boldsymbol{y}$;

(2) The signer calculates $(x_1,\mathrm{L}\ ,x_n)=\mathcal{Q}^{-1}(y_1,\mathrm{L}\ ,y_m)=\pi\mathrm{o}\mathcal{Q}^{\%}\mathrm{o}\pi^{-1}(y_1,\mathrm{L}\ ,y_m)$ and denotes the result $(x_1,\mathrm{L}\ ,x_n)$ as $\boldsymbol{x}$;

(3) The signer uses the private key $\mathcal{S}^{-1}$ to obtain $(v_1,\mathrm{L}\ ,v_n)=\mathcal{S}^{-1}(x_1,\mathrm{L}\ ,x_n)$ and remembers $(v_1,\mathrm{L}\ ,v_n)$ as $\boldsymbol{v}$.

The signature generation above is the same as that in the original model. $\boldsymbol{v}$ is called forward signature.

(4) The signer uses private key $\mathcal{G}$ to get $\mathcal{G}(x_1,\mathrm{L}\ ,x_n)=(g_1(x_1,\mathrm{L}\ ,x_n),\mathrm{L}\ ,g_n(x_1,\mathrm{L}\ ,x_n))=(g_1,\mathrm{L}\ ,g_n)$ and denotes it as $\boldsymbol{g}$;

(5) The signer uses $\mathcal{S}^{-1}$ of the private key $\mathcal{S}$ to obtain $\mathcal{S}^{-1}(\boldsymbol{g})=\mathcal{S}^{-1}\mathrm{o}\mathcal{G}(\boldsymbol{x})=(v_{g1},\mathrm{L}\ ,v_{gn})$ and denotes it as $\boldsymbol{v}_g$. $\boldsymbol{v}_g$ is the backward signature.

The concatenated $\boldsymbol{v}\|\boldsymbol{v}_g$ is the final signature of message $\mathcal{M}$.

3.3. The signature verification

(1) The verifier uses the signer's public key to calculate $\mathcal{P}(v_1,\mathrm{L}\ ,v_n)$ and verifies $\mathcal{P}(v_1,\mathrm{L}\ ,v_n)\overset{?}{=}(u_1,\mathrm{L}\ ,u_m)$. If it does, then continue with the next step, otherwise reject.

(2) The verifier takes the forward signature $(v_1,\mathrm{L}\ ,v_n)$ into $\mathcal{H}\mathrm{o}\mathcal{S}$ to get $\mathcal{H}\mathrm{o}\mathcal{S}(v_1,\mathrm{L}\ ,v_n)$, which denoted as $(h_1,\mathrm{L}\ ,h_n)$. The backward signature $(v_{g1},\mathrm{L}\ ,v_{gn})$ is substituted into the public key $\mathcal{H}\mathrm{o}\mathcal{G}^{-1}\mathrm{o}\mathcal{S}$ to obtain the result $\mathcal{H}\mathrm{o}\mathcal{G}^{-1}\mathrm{o}\mathcal{S}(v_{g1},\mathrm{L}\ ,v_{gn})$, which denoted as $(h_1',\mathrm{L}\ ,h_n')$. If $(h_1',\mathrm{L}\ ,h_n')$ and $(h_1,\mathrm{L}\ ,h_n)$ are equal, the signature is valid, otherwise the signature is invalid and rejected.

(3) The verifier substitutes respectively the backward signature $(v_{g1},\mathrm{L}\ ,v_{gn})$ and message $(u_1,\mathrm{L}\ ,u_m)$

into public key $\tilde{\mathcal{H}} \circ \mathcal{Q} \circ \mathcal{G}^{-1} \circ \mathcal{S}$ and $\tilde{\mathcal{H}} \circ \mathcal{T}^{-1}$ to obtain $\left(\tilde{h}_1, \ldots, \tilde{h}_m\right) = \tilde{\mathcal{H}} \circ \mathcal{Q} \circ \mathcal{G}^{-1} \circ \mathcal{S}\left(v_{g1}, \ldots, v_{gn}\right)$ and $\left(\tilde{h}_1, \ldots, \tilde{h}_m\right) = \tilde{\mathcal{H}} \circ \mathcal{T}^{-1}\left(u_1, \ldots, u_n\right)$ respectively. If the value $\left(\tilde{h}_1, \ldots, \tilde{h}_m\right)$ is equal to $\left(\tilde{h}_1, \ldots, \tilde{h}_m\right)$, then signature is valid and accepted, otherwise the signature is rejected.

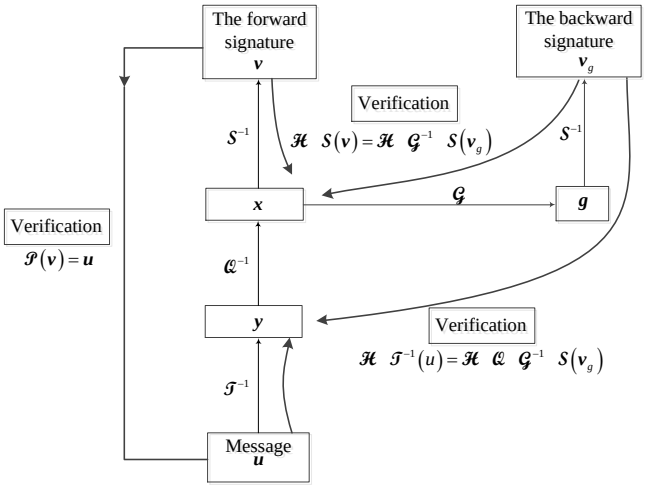

Figure 2. The improved signature model of multivariate public key cryptosystem.

3.4. Security analysis

Suppose the signature $v \| v_g$ is generated according to the above steps. Then we have

$$\mathcal{P}(v) = \mathcal{P}\left(\mathcal{S}^{-1} \circ \mathcal{Q}^{-1} \circ \mathcal{T}^{-1}\left(u_1, \ldots, u_m\right)\right) = \mathcal{P} \circ \mathcal{S}^{-1} \circ \mathcal{Q}^{-1} \circ \mathcal{T}^{-1}(u) = \mathcal{T} \circ \mathcal{Q} \circ \mathcal{S} \circ \mathcal{S}^{-1} \circ \mathcal{Q}^{-1} \circ \mathcal{T}^{-1}(u) = u,$$

$$S(v) = \left(x_1, \ldots, x_n\right) = \mathcal{G}^{-1} \circ \mathcal{S}\left(v_g\right) \text{ and } \mathcal{Q} \circ \mathcal{G}^{-1} \circ \mathcal{S}\left(v_g\right) = y = \mathcal{T}^{-1}(u).$$

The correctness of this algorithm is intuitively clear.

Claim 1: In the improved multivariate signature model, the probability of finding equivalent keys of a given public key is approaching 0 for some concrete trapdoor structure.

As is analyzed previously, the multivariate polynomial cryptographic system always has the characteristic of "equivalent key". That is the same public key corresponds to multiple private keys. Therefore, with the help of the key recovery attack, the attacker succeeded in forging signature without the correct private key $(\mathcal{T}, \mathcal{Q}, \mathcal{S})$. However even the attacker gets an equivalent private key $(\mathcal{T}', \mathcal{Q}', \mathcal{S}')$ in our proposed construction, the probability that he forges a signature is 0. A signature is valid in the improved model, only when it consist of a forward signature v and a backward signature v_g and it is verified by verification condition (1), (2) and (3) in Section 3.3. However it is

impossible for a signature followed by equivalent key. For a signature $\hat{\boldsymbol{v}}\|\hat{\boldsymbol{v}}_g$ recovered by an equivalent key $(\mathcal{T}', \mathcal{Q}', \mathcal{S}')$ through the key recovery attack, the forward part is denoted as $\hat{\boldsymbol{v}}$, and the backward part is denoted as $\hat{\boldsymbol{v}}_g$. We say it would still unable to pass verification condition 2 and 3. In condition 2, the public keys $\mathcal{H} \circ \mathcal{S}$ and $\mathcal{H} \circ \mathcal{Q}^{-1} \circ \mathcal{S}$ restrict the internal note information $\boldsymbol{x}$ for correct signature $\boldsymbol{v}\|\boldsymbol{v}_g$ and $\boldsymbol{x}$ is generated by correct private key $\mathcal{T}, \mathcal{S}$. Similarly, in condition 3, the public keys $\mathcal{H} \circ \mathcal{Q} \circ \mathcal{Q}^{-1} \circ \mathcal{S}$ and $\mathcal{H} \circ \mathcal{T}^{-1}$ restrict the internal note information $\boldsymbol{y}$ for correct signature $\boldsymbol{v}\|\boldsymbol{v}_g$ and $\boldsymbol{y}$ is generated by correct private key $\mathcal{T}$. However, the equality probability of the equivalent $\mathcal{T}'$ and the right $\mathcal{T}$ is $p(\mathcal{T}' = \mathcal{T}) = 1/q^m$. Similarly, the equality probability of the equivalent $(\mathcal{T}', \mathcal{S}')$ and the right $(\mathcal{T}, \mathcal{S})$ is $p(\mathcal{T}' = \mathcal{T} \wedge \mathcal{S}' = \mathcal{S}') = 1/q^{mn}$. Moreover, if an attacker randomly guesses a forward signature $\hat{\boldsymbol{v}}$ and a backward signature $\hat{\boldsymbol{v}}_g$, the probability of correct guess for $p(\hat{\boldsymbol{v}} = \boldsymbol{v} \wedge \hat{\boldsymbol{v}}_g = \boldsymbol{v}_g)$ is $\frac{1}{q^{2n}}$.

Therefore the improved model can effectively help multivariate scheme to resist the key recovery attack and forking signature.

4. Comparative analysis of HFE in the original model and the improved model

HFE is one classical multivariate polynomial cryptosystem [26]. However it was broken by recovering the secret key from the public key by linearization technique, which is belong to key recovery attack [35].

In this section, by comparing HFE scheme in the original model and the improved model, we shows that the new improved model enhance the security of the HFE scheme and help HFE resist and key recovery attack of the linearization technique.

4.1. HFE scheme

Let F be an q order finite field and E be a n-th power extension field of F. The isomorphic mapping $\pi : \mathrm{E} \to \mathrm{F}^n$ is defined from the extended domain to vector space. The central map of HFE is homogeneous polynomials (the lower degree monomials can be ignored for they have no impact on security):

$$\mathcal{Q}(X) := \sum_{\substack{0 \le i,j \le d \\ q^i + q^j \le d}} C_{i,j} X^{q^i + q^j}$$

where $i, j \in \mathrm{N}$, $d \in \mathrm{N}$. The second-order coefficients $C_{i,j} \in \mathrm{E}$ are randomly selected. The degree q^i and q^j must be less than some parameter d to be resolved. Then central map $\mathcal{Q}(x_1, \mathrm{L}, x_n)$ is quadratic mapping from F to F :

$$\mathcal{Q}(x_1, \mathrm{L}, x_n) = (q_1(x_1, \mathrm{L}, x_n), \mathrm{L}, q_n(x_1, \mathrm{L}, x_n)) = \pi \circ \mathcal{Q} \circ \pi^{-1}(x_1, \mathrm{L}, x_n).$$

$\mathcal{P} = \mathcal{T} \circ \pi \circ \mathcal{Q} \circ \pi^{-1} \circ \mathcal{S}(\boldsymbol{x}) = \mathcal{T} \circ \mathcal{Q} \circ \mathcal{S}(\boldsymbol{x})$ is public key. $\mathcal{T}$ and $\mathcal{S}$ are private keys.

4.2. Key recovery attack on HFE scheme under original model

Kipins and Shamir broke the HFE scheme using linearization technique by key recovery attack, and the idea is given as follows [35,36].

We take a set of εm^2 quadratic equations in m variables x_1, L, x_m, where ε is constant. It can be rewritten as a new set of εm^2 linear equations in the approximately $m^2/2$ new variables $y_{ij} = x_i x_j$, where $i \le j$. Then for any 4-tuple $x_a x_b x_c x_d$ of indices $1 \le a \le b \le c \le d \le m$, it is parenthesized in three different ways:

$$(x_a x_b)(x_c x_d) = (x_a x_c)(x_b x_d) = (x_a x_d)(x_b x_c) \Rightarrow y_{ab} y_{cd} = y_{ac} y_{bd} = y_{ad} y_{bc}.$$

Then there are about $m^4/4!$ different ways to choose from the sorted 4-tuples of distinct indices, and each choice gives rise to 2 equations. Thus there are about $m^4/12$ quadratic equations in the $m^2/2$ y_{ij} variables, and these equations are linearly independent. By replacing each one of the y_{ij} variables via its parametric representation as a linear combination of the new z_k variables, the number of variables is decreased to $(1/2 - \varepsilon)m^2$. The new $m^4/12$ quadratic equations in the new $(1/2 - \varepsilon)m^2$ z_i variables can be linearized again by replacing each product $z_i z_j$ for $i \le j$ by new variables v_{ij}, which is called the relinearization technique and is belong to key recover attack. Then the new system has $m^4/12$ linear equations in $\left((1/2 - \varepsilon)m^2\right)^2/2$ variables v_{ij}.

The relinear process is summarized as follows.

Table 1. The process of the relinearization technique.

The number of the equations	The number of the variables	Variables
εm^2	m	$x_1,\mathrm{L}\ ,x_m$
$m^4/12$	$m^2/2$	$y_{ij}=x_ix_j$
$m^4/12$	$(1/2-\varepsilon)m^2$	$z_k=y_{ij}$
$m^4/12$	$\left((1/2-\varepsilon)m^2\right)^2/2$	$v_{ij}=z_iz_j$

When $m^4/12\geq\left((1/2-\varepsilon)m^2\right)^2/2$, that is $\varepsilon\geq 1/2-1/\sqrt{6}\approx 0.1$, the linear system is resolved uniquely by Gauss linearization. Therefore, HFE Scheme under original model was broken by the key recovery attack.

4.3. HFE signature scheme under the improved model

In the improved signature model, as analysis in Section 2.4, for the same message $(u_1,\mathrm{L}\ ,u_m)$, the signature changes from the original to two parts, $v_1,\mathrm{L}\ ,v_n$ and $v_{g1},\mathrm{L}\ ,v_{gn}$. When verifying that whether the $\mathcal{P}_{Alice}(v_1,\mathrm{L}\ ,v_n)$ is equal to $(u_1,\mathrm{L}\ ,u_n)$, namely using the original public key $\mathcal{P}_{Alice}$, it is necessary to verify that whether the $\mathcal{H}\mathrm{o}\mathcal{G}^{-1}\mathrm{o}\mathcal{S}_{Alice}(v_1,\mathrm{L}\ ,v_n)$ associated with the private key is equal to the $\mathcal{H}\mathrm{o}\mathcal{S}_{Alice}(v_{g_1},\mathrm{L}\ ,v_{g_n})$ and whether the $\mathcal{H}\mathrm{o}\mathcal{T}^{-1}_{Alice}(u_1,\mathrm{L}\ ,u_n)$ is equal to $\mathcal{H}\mathrm{o}\mathcal{Q}\mathrm{o}\mathcal{G}^{-1}\mathrm{o}\mathcal{S}_{Alice}(v_{g1},\mathrm{L}\ ,v_{gn})$. This shows that only when all three conditions are verified, $v_1,\mathrm{L}\ ,v_n\|v_{g1},\mathrm{L}\ ,v_{gn}$ can be obtained. Thus it is a valid signature. That is to say, the verification under the new model involves not only the message $\boldsymbol{u}$ and signature $\boldsymbol{v}$, but also the verification of the internal node information. And according the recommended choice, such as q=GF$(2)^{128}$ and suitable parameters m and n for HFE in [35], the probabilities finding the equivalent keys in Section 2.4 are all close to 0.

Therefore, the improved model is guaranteed that each signature is generated by the correct private key of the legitimate user, which prevents the equivalent key from recovering and signature from forging by the key recovery attack.

4.4. Performance analysis

4.4.1. Computation complexity

As shown in the original model, the kernel polynomials q_1,L q_m are m polynomials in n variables of degree 2, since for any integer d, x a x^{q^d} is a linear function of F^n a F^n [26]. In the original model, the time of signature generation include the inverse of affine transformation $\mathcal{S}$, the inverse of central mapping $\mathcal{Q}$ and the inverse of affine transformation $\mathcal{T}$, so the time complexity is ($O\left[m^2 + d \cdot \frac{mn(n-1)}{2} + n^2\right]$). Similarly, the time complexity of the verification process is ($O\left[m\left(\frac{n(n-1)}{2} + n + 1\right)\right]$). In the improved model, the signature generation of HFE has the same time complexity as in the original model. However, the time of signature verification has a little more than that in original model, for there are two additional verification conditions. Thus the total time complexity of the verification is $O\left[m\left(\frac{n(n-1)}{2} + n + 1\right) + n + m\right]$. The comparison of HFE in the original model and the improved model are as Table 2.

Table 2. The comparison of computation complexity for HFE in the original model and the improved Model.

Scheme	The signature generation	The signature verification
HFE in the original model	$O\left[m^2 + d \cdot \frac{mn(n-1)}{2} + n^2\right]$	$O\left[m\left(\frac{n(n-1)}{2} + n + 1\right)\right]$
HFE in the improved model	$O\left[m^2 + d \cdot \frac{mn(n-1)}{2} + n^2\right]$	$O\left[m\left(\frac{n(n-1)}{2} + n + 1\right) + n + m\right]$

Then we easily can get the computation complexity for some parameter, such as $m = n = 128$ or 160 [26].

4.4.2. Experimental results

The evaluation is conducted through experiment assessing the time cost of the proposed scheme on a computer with Windows7 Intel i5-4570S-2.90GHz CPU and 8-GB RAM. For the convenience of comparative analysis, we set m=n in experiment. All results presented here are the average value in 100 different messages. The cost of signature depends on the computation of $\mathcal{Q}^{-1}$. With the help of Magma V2.12-16, we take efficient FM algorithm. Consider the parameter d is not be too big and

it will be out of our memory or system resources for larger input parameter, we list some corresponding signature and verification time for about $2^2 \le q \le 2^8$, $4 \le n \le 64$ and $3 \le d \le 7$ in Table 3. To achieve higher security requirements, larger parameters can be taken.

Table 3. The average signature and verification time for HFE in 1000 messages.

Model	q	n	d	signature time(s)	verification time(s)
HFE in	4	4	3	0.001	0.001
original	8	4	3	0.002	0.002
model	16	4	3	0.041	0.003
	32	4	3	0.229	0.005
	64	4	3	1.792	0.009
	128	4	3	8.903	0.014
	256	4	3	64.314	0.016
	8	8	3	0.012	0.003
	8	16	3	0.19	0.043
	8	32	3	5.473	1.285
	8	64	3	220.149	36.785
HFE in	4	4	3	0.002	0.002
improved	8	4	3	0.002	0.006
model	16	4	3	0.041	0.094
	32	4	3	0.248	0.531
	64	4	3	1.681	3.570
	128	4	3	8.700	19.589
	256	4	3	63.781	120.097
	8	8	3	0.014	0.022
	8	16	3	0.264	0.191
	8	32	3	7.705	4.047
	8	64	3	367.086	132.242

The speed of verification is faster than the signature in these two models, since the signature needs to compute the α^{-1} while the verification is only to compute common modulo additions and multiplications on finite field. The parameter q, n and d in HFE takes a large number, then the overload of signature or verification will be very large. Both signature time and verification time in improved model is increased compared with those in the original model. It is easy to understand that the small-scale increase of parameters leads to the signature and verification time in a highly non-linear fashion. This basically conforms to the nonlinear properties of central map of multivariate polynomials cryptosystem.

To provide the detailed differences of small values, we give two classifications by parameters according the Table 3 and evaluate the logarithm of these times in following figures.

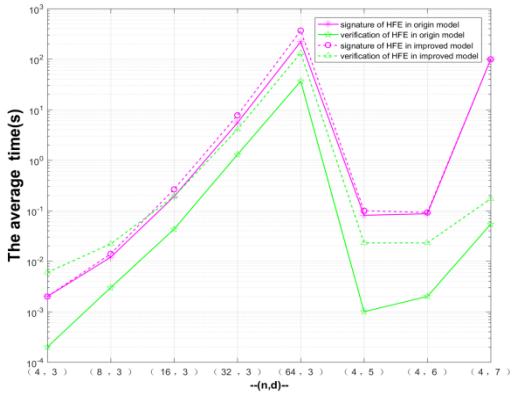

Figure 3. The comparison of HFE in original and improved model with $q = 2^3$.

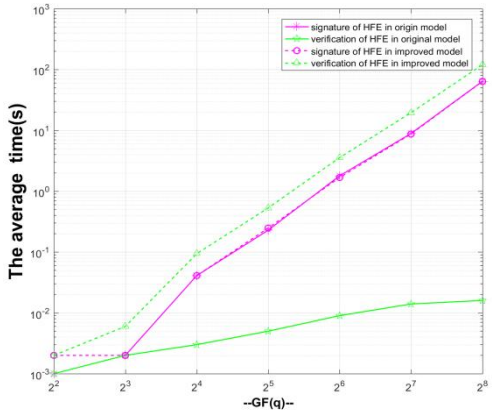

Figure 4. The comparison of HFE in original and improved model with $n = 4, d = 3$.

Fix $q = 2^3$, the comparing results with different degree and number of equations (n, d) is presented in Figure 3. It shows that the more equations or degrees, the greater the consumption. Especially, when n is double, the signature and verification time is increased to several dozen times in these two models. It is similar when the degree d is large.

Fix $n = 4, d = 3$, the comparing results with different size of finite field q is presented in Figure 4. We also conclude that the larger size of finite field, the greater the consumption, furthermore in the form of nonlinear approach to exponential growth. The verification time in the improved model is increased much more than the original model. For there are three verification conditions in the improved model while only one verification condition in the original model. However, the indicators of signature time are not very different from each other, and no significant difference is shown.

5. Conclusions

The existing signature model of multivariate system does not take the potential hazard of the key recovery attack at the initial design into account. To overcome the defect, this paper proposes an improved signature model. In the new model, a strengthening public key verification progress of verifying the internal information is proposed to inhibit the forged signature brought with the key recovery attack effectively. Finally, we take the classical scheme HFE as an example to illustrate that the new model can effectively resist key recovery attacks. It provides a useful supplement to the design and research of secure digital signature schemes in the quantum age.

Acknowledgments

This work is supported by National Key R&D Program of China (No. 2017YFB0802000), the National Natural Science Foundation of China (61572303, 61772326,61802241, 61802242), National Cryptography Development Fund during the 13th Five-year Plan Period (MMJJ20180217), the Foundation of State Key Laboratory of Information Security (2017-MS-03) and the Doctoral Scientific Fund Project of Shaanxi University of Science & Technology of China (No. BJ11-12).

Conflict of interest

All authors declared that we have no conflicts of interest to this work.

References

1. A. Huelsing, D. Butin, S. Gazdag, et al., XMSS: eXtended Merkle Signature Scheme, RFC 8391 (May 2018). Available from: https://tools.ietf.org/html/rfc8391.
2. R. E. Bansarkhani and R. Misoczki, G-Merkle: A hash-based group signature scheme from standard assumptions, *PQCrypto*, (2018), 441–463.
3. Y. Ashino and R. Sasaki, Proposal of digital forensic system using security device and hysteresis signature, *IEEE Compt. Soc.*, **2** (2008), 3–7.
4. S. Tezuka, R. Uda and K. Okada, ADEC: Assured deletion and verifiable version control for cloud storage, *AINA*, **11** (2012), 23–30.
5. Shor and W. Peter, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SICOMP*, **41** (1999), 1484–1509.
6. J. Ding and B. Yang, Multivariate public key cryptography, *PQCrypto*, (2008), 193–234.
7. M. Garay and D. Johnson, Computers and intractability: a guide to the theory of NP-Completeness, New York, USA, *W.H. Freeman and Company*, 1979.
8. A. Kipnis, J. Patarin and L. Goubin, Unbalanced oil and vinegar signature schemes, *Eurocrypt*, (1999), 206–222.
9. J. Ding and D. Schmidt, Rainbow, a new multivariable polynomial signature scheme, *Appl. Cryptogr. Net. Secur.*, (2005), 164–175.
10. M. S. Chen, A. Hülsing, J. Rijneveld, et al., From 5-pass MQ-based identification to MQ-based signatures, International Conference On, Part II. Springer-Verlag New York, Inc., (2016), 135–165.

11. A. Petzoldt, A. Szepieniec and M. S. E. Mohamed, A practical multivariate blind signature scheme, International Conference on Financial Cryptography & Data Security. Springer, Cham, (2017), 437–454.
12. Y. Hashimoto, Key recovery attacks on multivariate public key cryptosystems derived from quadratic forms over an extension field, *IEICE T. Fund. Electr.*, **100** (2017), 18–25.
13. C. Wolf and B. Preneel, Large superfluous keys in multivariate quadratic asymmetric systems, *PKC*, (2005), 275–287.
14. C. Wolf and B. Preneel, Equivalent keys in HFE, C^*, and variations, *Mycrypt*, (2005), 33–49.
15. J. C. Faugère, D. Gligoroski, L. Perret, et al., A polynomial-time key-recovery attack on MQQ cryptosystems, IACR International Workshop on Public Key Cryptography. Springer, Berlin, Heidelberg, (2015), 150–174.
16. N. Courtois, A. Klimov, J. Patarin, et al., Efficient algorithms for solving overdefined systems of multivariate polynomial equations, *Proc. Eurocrypt*, (2000), 392–407.
17. A. Biryukov, C. D. Christophe, B. An, et al., A toolbox for cryptanalysis: Linear and affine equivalence algorithms, *Lect. Notes Comput. Sci.*, (2003), 33–50.
18. Y. H. Hu, L. C. Wang, C. Y. Chou, et al., Similar keys of multivariate quadratic public key cryptosystems, International Conference on Cryptology & Network Security. Springer-Verlag, (2005), 211–222.
19. C. Bouillaguet, P. A. Fouque, A. Joux, et al., A family of weak keys in HFE and the corresponding practical key-recovery, *J. Math. Cryptol.*, **5** (2012), 247–275.
20. H. Wang, H. Zhang and S. Tang, Key recovery on several matrix public-key encryption schemes, *IET Inform. Secur.*, **10** (2016), 152–155.
21. D. Cabarcas, D. Smith-Tone and J. A. Verbel, Key recovery attack for ZHFE, International Workshop on Post-quantum Cryptography. Springer, Cham, (2017), 289–308.
22. J. Porras, J. Baena and J. Ding, ZHFE, a new multivariate public key encryption scheme, International Workshop on Post-Quantum Cryptography, (2014), 229–245.
23. A. Petzoldt, M. S. Chen , J. Ding, et al., HMFEv-an efficient multivariate signature scheme, International Workshop on Post-Quantum Cryptography. Springer, Cham, (2017), 205–223.
24. L. Bettale, J. C. Faugère and L. Perret, Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic, *Design. Code. Cryptogr.*, **69** (2013), 1–52.
25. J. Vates and D. Smith-Tone, Key recovery attack for all parameters of HFE-, *PQCrypto*, (2017), 272–288.
26. J. Patarin, Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms, *Eurocrypt*, (1996), 33–48.
27. A. Szepieniec, W. Beullens and B. Preneel, MQ signatures for PKI, *PQCrypto*, (2017), 224–240.
28. A. Szepieniec and B. Preneel, Block-anti-circulant unbalanced oil and vinegar, (2019). Available from: https://eprint.iacr.org/2019/046.pdf.
29. D. J. Bernstein, J. Buchmann and E. Dahmen, Introduction to post-quantum cryptography, *Post-Quantum Cryptography*, 1st ed. New York, USA: Springer, Heidelberg, 2010.
30. Y. Hashimoto, Multivariate public key cryptosystems, *Math. Model.r Next-Gen. Cryptogr.*, **29** (2017), 17–42.
31. H. Gilbert, J. Plût, and J. Treger, Key-recovery attack on the ASASA cryptosystem with expanding S-boxes, Advances in Cryptology-CRYPTO 2015. Springer Berlin Heidelberg, (2015), 475–490.

32. E. Thomae, About the security of multivariate quadratic public key schemes, Ph.D thesis, Ruhr-University in Bochum, Germany, 2013.
33. A. Petzoldt, Selecting and reducing key sizes for multivariate cryptography, Ph.D thesis, Technische Universität Darmstadt in Germany, 2013.
34. C. Park, Cryptanalysis of matrix-based UOV, *Finite Fields Th. App.*, **50** (2018), 209–221.
35. A. Kipnis and A. Shamir, Cryptanalysis of the HFE public key cryptosystem by relinearization, *Proc. Crypto*, (1999), 19–30.
36. Y. Hashimoto, On the security of HMFEv, (2017). Available from: https://www.researchgate.net/publication/318543302_On_the_security_of_HMFEv.

AIMS Press