(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 October 2016 (06.10.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/155565 A1

(51) International Patent Classification:
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/CN2016/077293

(22) International Filing Date:
25 March 2016 (25.03.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/139,935 30 March 2015 (30.03.2015) US

(72) Inventor; and
(71) Applicant : **DING, Jintai** [CN/CN]; North Campus 28-203, University of Science and Technology of China, No.96, JinZhai Road, Baohe District, Hefei, Anhui 230026 (CN).

(74) Agent: **BEYOND TALENT PATENT AGENT FIRM**; Room 1202, Kuntai Building, #10 Chaoyangmenwai Str., Chaoyang District, Beijing 100020 (CN).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report (Art. 21(3))*

WO 2016/155565 A1

(54) **Title**: IMPROVEMENTS ON MULTIVARIATE DIGITAL SIGNATURE SCHEMES BASED ON HFEV- AND NEW APPLICATIONS OF MULTIVARIATE DIGITAL SIGNATURE SCHEMES FOR WHITE-BOX ENCRYPTION

(57) **Abstract**: We present new designs to choose the parameter sets for more efficient HFEv-based signature schemes. The key method is to reduce the degree of the central HFEv-polynomial while, at the same time, increasing the number of Vinegar variables and Minus equations. The new design speeds up the signature generation process by two orders of magnitude (hundreds of times) compared to QUARTZ. We present also new methods to use multivariate signature schemes to build a white box encryption scheme. This technique is applicable to all existing multivariate signature designs including the HFEV-design and the improvements.

Description

Title: Improvements on Multivariate Digital Signature Schemes Based on HFEv- and New Applications of Multivariate Digital Signature Schemes for White-box Encryption

BACKGROUND

[**1**] This invention is related to the construction of more efficient multivariate public key signature schemes using the HFEv- idea and new applications of multivariate digital signature schemes for white-box encryption.

[**2**] Cryptographic techniques are an essential tool to guarantee the security of communication in modern society. Today, the security of nearly all of the cryptographic schemes used in practice is based on number theoretic problems such as factoring large integers and solving discrete logarithms. The best known schemes in this area are RSA [27], DSA [19] and ECC. However, schemes like these will become insecure as soon as large enough quantum computers arrive. The reason for this is Shor's algorithm [28], which solves number theoretic problems like integer factorization and discrete logarithms in polynomial time on a quantum computer. Therefore, one needs alternatives to those classical public key schemes, based on hard mathematical problems not affected by quantum computer attacks.

[**3**] Besides lattice, code and hash based cryptosystems, multivariate cryptography is one of the main candidates for this [1]. Multivariate schemes are in general very fast and require only modest computational resources, which makes them attractive for the use on low cost devices like smart cards and RFID chips [3, 4]. Additionally, at least in the area of digital signatures, there exists a large number of practical multivariate schemes [12, 17].

[**4**] In 2001, Patarin and Courtois proposed a multivariate signature scheme called QUARTZ [24], which is based on the concept of HFEv-. While QUARTZ produces very short signatures (128 bit), the signature generation process is very slow (at the time about 11 seconds per signature [4]). The main reason for this is the use of a high degree HFE polynomial (for QUARTZ this degree is given by $D = 129$), which makes the inversion of the central map very costly.

[**5**] At the time of the design of the QUARTZ scheme, very little was known about the complexity of algebraic attacks against the HFE family of systems, in particular, the HFEv- schemes. Therefore, the authors of QUARTZ could not base their parameter choice on theoretical foundations.

[**6**] Recently, there has been a fundamental breakthrough in terms of understanding the behavior of algebraic attacks on the HFE family of systems [9, 10, 13], which enables us to substantially improve the original design of QUARTZ without weakening the security of the scheme.

BRIEF SUMMARY OF THE INVENTION

[**7**] First, we present new principles for the parameter choice of HFEv- based signature schemes, which allow us to improve the efficiency of the scheme drastically. Using the formula we have, we give examples at the low (80-bit) and high (112+-bit) security levels. The key

method of this is to reduce the degree of the central HFEv- polynomial while, at the same time, increasing the number of Vinegar variables and Minus equations.

[8] Under state-of-the-art theoretical and experimental analysis, we show that these modifications do not weaken the security of the scheme, compared to conservative choices like the original QUARTZ design. The new design (named Gui) speeds up the signature generation process by two orders of magnitude (hundreds of times) compared to QUARTZ, and has a comparable performance to standard signature schemes like RSA and ECDSA.

[9] We present also new methods to use multivariate signature schemes to build a white box encryption scheme. This technique is applicable to all existing multivariate signature schemes including the HFEV- design [24] and the improvements above.

DETAILED DESCRIPTION OF THE INVENTION

1.1 The improvements on the signature schemes of the $HFEv-$ type

[10] The basic objects of multivariate cryptography are systems of multivariate quadratic polynomials.

[11] The security of multivariate schemes is based on the

MQ Problem: Given m multivariate quadratic polynomials $p^{(1)}(\mathbf{x}), \ldots, p^{(m)}(\mathbf{x})$ in n variables, find a vector $\bar{\mathbf{x}} = (\bar{x}_1, \ldots, \bar{x}_n)$ such that $p^{(1)}(\bar{\mathbf{x}}) = \ldots = p^{(m)}(\bar{\mathbf{x}}) = 0$.
The MQ problem (for $m \approx n$) is proven to be NP-hard even for quadratic polynomials over the field GF(2) [16].

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

[13] This invention is related to multivariate signature schemes of the BigField family. For this type of multivariate schemes, the map $\mathcal{F}$ is a specially chosen easily invertible map over a degree n extension field $\mathbb{E}$ of $\mathbb{F}$. One uses an isomorphism $\Phi : \mathbb{F}^n \to \mathbb{E}$ to transform $\mathcal{F}$ into a quadratic map

$$\bar{\mathcal{F}} = \Phi^{-1} \circ \mathcal{F} \circ \Phi \tag{1}$$

from $\mathbb{F}^n$ to itself. The public key of the scheme is therefore given by

$$\mathcal{P} = \mathcal{S} \circ \bar{\mathcal{F}} \circ \mathcal{T} = \mathcal{S} \circ \Phi^{-1} \circ \mathcal{F} \circ \Phi \circ \mathcal{T} : \mathbb{F}^n \to \mathbb{F}^n. \tag{2}$$

The standard signature generation and verification process of a multivariate BigField scheme works as shown in Figure 1.

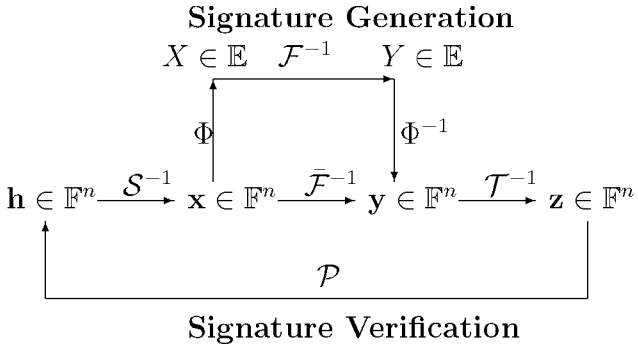


FIGURE 1. General workflow of BigField schemes

[**14**] *Signature generation*: To sign a message $\mathbf{h} \in \mathbb{F}^n$, one computes recursively $\mathbf{x} = \mathcal{S}^{-1}(\mathbf{h}) \in \mathbb{F}^n$, $X = \Phi(\mathbf{x}) \in \mathbb{E}$, $Y = \mathcal{F}^{-1}(X) \in \mathbb{E}$, $\mathbf{y} = \Phi^{-1}(Y) \in \mathbb{F}^n$ and $\mathbf{z} = \mathcal{T}^{-1}(\mathbf{y})$. The signature of the message $\mathbf{h}$ is $\mathbf{z} \in \mathbb{F}^n$.

[**15**] *Verification*: To check the authenticity of a signature $\mathbf{z} \in \mathbb{F}^n$, one simply computes $\mathbf{h}' = \mathcal{P}(\mathbf{z}) \in \mathbb{F}^n$. If $\mathbf{h}' = \mathbf{h}$ holds, the signature is accepted, otherwise rejected. [**16**] A widely known example for a multivariate scheme of the BigField family is the HFE (Hidden Field Equations) cryptosystem. For this scheme, the central map $\mathcal{F}$ has the form

$$\mathcal{F}(X) = \sum_{i,j=0}^{q^i+q^j \leq D} \alpha_{i,j} \cdot X^{q^i+q^j} + \sum_{i=1}^{q^i \leq D} \beta_i \cdot X^{q^i} + \gamma \tag{3}$$

with coefficients $\alpha_{i,j}$, β_i and $\gamma \in \mathbb{E}$. Due to the special structure of $\mathcal{F}$, the map $\bar{\mathcal{F}} : \Phi^{-1} \circ \mathcal{F} \circ \Phi$ is a multivariate quadratic map over the vector space $\mathbb{F}^n$. Furthermore, if D is not too large, $\mathcal{F}$ can be efficiently inverted using Berlekamp's algorithm.

[**17**] This basic idea was patented under United States Patent 5,790,675 by Jacques Patarin with the title "Cryptographic communication process".

[**18**] Two widely used variations of multivariate BigField schemes are the Minus variation and the use of additional (Vinegar) variables.

[**19**] **Minus-Variation**: The idea of this variation is to remove a small number of equations from the public key. The Minus-Variation was first used in schemes like SFLASH [25] to prevent Patarins Linearization Equations attack [23] against the Matsumoto-Imai cryptosystem [20].

[**20**] **Vinegar-Variation**: The idea of this variation is to parametrize the central map $\mathcal{F}$ by adding (a small set of) additional (Vinegar) variables. In the context of multivariate BigField schemes, the Vinegar variation can be used to increase the security of the scheme against direct and rank attacks.

[**21**] HFEv- is an HFE variant optimized for signatures, which combines the basic HFE scheme with the Minus and the Vinegar-Modification.

[**22**] Let $\mathbb{F} = \mathbb{F}_q$ be a finite field with q elements and $\mathbb{E}$ be a degree n extension field of $\mathbb{F}$. Furthermore, we choose integers D, a and v. Let Φ be the canonical isomorphism between $\mathbb{F}^n$ and $\mathbb{E}$, i.e.

$$\Phi(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i \cdot X^{i-1}. \tag{4}$$

The central map $\mathcal{F}$ of the HFEv- scheme is a map from $\mathbb{E} \times \mathbb{F}^v$ to $\mathbb{E}$ of the form

$$\mathcal{F}(X) = \sum_{i,j=0}^{q^i+q^j \leq D} \alpha_{i,j} \cdot X^{q^i+q^j} + \sum_{i=1}^{q^i \leq D} \beta_i(v_1, \ldots, v_v) \cdot X^{q^i} + \gamma(v_1, \ldots, v_v), \tag{5}$$

with $\alpha_{i,j} \in \mathbb{E}$, $\beta_i : \mathbb{F}^v \to \mathbb{E}$ being linear and $\gamma : \mathbb{F}^v \to \mathbb{E}$ being a quadratic function. Due to the special form of $\mathcal{F}$, the map $\bar{\mathcal{F}} = \Phi^{-1} \circ \mathcal{F} \circ \Phi$ is a quadratic polynomial map from $\mathbb{F}^{n+v}$ to $\mathbb{F}^n$. To hide the structure of $\bar{\mathcal{F}}$ in the public key, one combines it with two affine (or linear) maps $\mathcal{S} : \mathbb{F}^n \to \mathbb{F}^{n-a}$ and $\mathcal{T} : \mathbb{F}^{n+v} \to \mathbb{F}^{n+v}$ of maximal rank.

[**23**] The *public key* of the scheme is the composed map $\mathcal{P} = \mathcal{S} \circ \bar{\mathcal{F}} \circ \mathcal{T} : \mathbb{F}^{n+v} \to \mathbb{F}^{n-a}$, the *private key* consists of $\mathcal{S}$, $\mathcal{F}$ and $\mathcal{T}$.

[**24**] *Signature generation*: To generate a signature for a message $\mathbf{h} \in \mathbb{F}^{n-a}$, the signer performs the following three steps.

(1) Compute a preimage $\mathbf{x} \in \mathbb{F}^n$ of $\mathbf{h}$ under the affine map $\mathcal{S}$.
(2) Lift $\mathbf{x}$ to the extension field $\mathbb{E}$ (using the isomorphism Φ). Denote the result by X.
Choose random values for the Vinegar variables $v_1, \ldots, v_v \in \mathbb{F}$ and compute $\mathcal{F}_V = \mathcal{F}(v_1, \ldots, v_v)$.
Solve the univariate polynomial equation $\mathcal{F}_V(Y) = X$ by Berlekamp's algorithm and compute $\mathbf{y}' = \Phi^{-1}(Y) \in \mathbb{F}^n$.
Set $\mathbf{y} = (\mathbf{y}'||v_1|| \ldots ||v_v)$.
(3) Compute the signature $\mathbf{z} \in \mathbb{F}^{n+v}$ by $\mathbf{z} = \mathcal{T}^{-1}(\mathbf{y})$.

[**25**] *Signature verification*: To check the authenticity of a signature $\mathbf{z} \in \mathbb{F}^{n+v}$, one simply computes $\mathbf{h}' = \mathcal{P}(\mathbf{z}) \in \mathbb{F}^{n-a}$. If $\mathbf{h}' = \mathbf{h}$ holds, the signature is accepted, otherwise rejected.

[**26**] QUARTZ is a multivariate signature scheme designed by Patarin and Courtois in [24]. It is an HFEv- based signature scheme with a specially designed signature generation process to enable secure short signatures of length 128 bit.

[**27**] Patarin and Courtois suggested the following parameters for QUARTZ:

$$(\mathbb{F}, n, D, a, v) = (\mathrm{GF}(2), 103, 129, 3, 4).$$

Due to this choice, the public key $\mathcal{P}$ of QUARTZ is a quadratic map from $\mathbb{F}^{107}$ to $\mathbb{F}^{100}$. The public key size of QUARTZ is 71 kB, the private key size 3 kB.
To avoid birthday attacks, Patarin and Courtois developed a special procedure for the signature generation process of QUARTZ. Roughly spoken, one computes four HFEv- signatures (for the messages $\mathbf{h}$, $\mathcal{H}(\mathbf{h}||0x00)$, $\mathcal{H}(\mathbf{h}||0x01)$ and $\mathcal{H}(\mathbf{h}||0x02)$) and combines them to a single 128 bit signature of the message $\mathbf{h}$. Analogously, during the signature verification process, one has to use the public key $\mathcal{P}$ four times.

[**28**] Security: Despite of its rather complicated signature generation process, breaking the QUARTZ scheme is still equivalent to breaking the underlying HFEv- scheme. The most important attacks against this scheme are

- the MinRank attack and
- direct algebraic attacks.

[**29**] The MinRank attack on HFE: We first describe the attack of Kipnis and Shamir [18] against the HFE cryptosystem. For the simplicity of our description we restrict ourselves to homogeneous maps $\mathcal{F}$ and $\mathcal{P}$.

[30] The key observation of the attack is to lift the maps $\mathcal{S}$, $\mathcal{T}$ and $\mathcal{P}$ to functions $\mathcal{S}^\star$, $\mathcal{T}^\star$ and $\mathcal{P}^\star$ over the extension field $\mathbb{E}$. Since $\mathcal{S}$ and $\mathcal{T}$ are linear maps, $\mathcal{S}^\star$ and $\mathcal{T}^\star$ have the form

$$\mathcal{S}^\star(X) = \sum_{i=1}^{n-1} s_i \cdot X^{q^i} \quad \text{and} \quad \mathcal{T}^\star(X) = \sum_{i=1}^{n-1} t_i \cdot X^{q^i}, \tag{6}$$

with coefficients s_i and $t_i \in \mathbb{E}$. The function $\mathcal{P}^\star$ can be expressed as

$$\mathcal{P}^\star(X) = \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} p_{ij}^\star X^{q^i+q^j} = \underline{X} \cdot P^\star \cdot \underline{X}^T, \tag{7}$$

where $P^\star = [p_{ij}^\star]$ and $\underline{X} = (X^{q^0}, X^{q^1}, \ldots, X^{q^{n-1}})$. Due to the relation $\mathcal{P}^\star(X) = \mathcal{S}^\star \circ \mathcal{F} \circ \mathcal{T}^\star(X)$ we get $\mathcal{S}^{\star\,-1} \circ \mathcal{P}^\star(X) = \mathcal{F} \circ \mathcal{T}^\star(X)$ and

$$\tilde{P} = \sum_{k=0}^{n-1} s_k \cdot G^{\star k} = W \cdot F \cdot W^T \tag{8}$$

with ${g_{ij}^\star}^k = ({p^\star}_{i-k,j-k})^{q^k}$, $w_{ij} = s_{j-i \bmod n}^{q^i}$ and F being the $n \times n$ matrix representing the central map $\mathcal{F}$. Note that, due to the special structure of $\mathcal{F}$, the only non zero entries in the matrix F are located in the upper left $r \times r$ submatrix ($r = \lfloor \log_q D - 1 \rfloor + 1$).
Since the rank of the matrix $W \cdot F \cdot W^T$ is less or equal to r, we can determine the coefficients s_k of equation (8) by solving an instance of the MinRank problem.

[31] In the setting of HFEv-, the rank of this matrix can, for odd characteristic, be bounded from above by [13]

$$\mathrm{Rank}(\widetilde{P}) \leq r + a + v. \tag{9}$$

Under the assumption that the vinegar maps β_i look like random functions, we find that this bound is tight.

[32] For fields of even characteristic we eventually have to decrease this rank by 1, since over those fields, the matrix $\widetilde{P}$ is always of even rank. The complexity of the MinRank attack against HFEv- schemes is therefore given roughly by

$$\mathrm{Complexity}_{\mathrm{MinRank}} = \mathcal{O}(q^{n\cdot(r+v+a-1)} \cdot (n-a)^3). \tag{10}$$

[33] For the HFE family of schemes, the direct attack, namely the attack by directly solving the public equation $\mathcal{P}(\mathbf{z}) = \mathbf{h}$ by an algorithm like XL or a Gröbner basis method such as F_4 [14] is a major concern due to which happened to HFE challenge 1 [15]. At the time of the design of the QUARTZ scheme, very little was known theoretically about the complexity of algebraic attacks against the HFE family of systems, in particular, the HFEv- schemes. The authors of QUARTZ did not actually give an explanation for their selection of the parameters and therefore the parameter selection of their scheme was not supported by theoretical results. We need to point out that, as has been shown by experiments [21], the public systems of HFEv- can be solved significantly easier than random systems.

[34] Recently, there has been a fundamental breakthrough in terms of understanding how algebraic attacks on the HFE family of systems work [9, 10, 13]. In particular, we now have a solid insight what happens in the case of HFEv-. An upper bound for the degeneration

degree of a Gröbner Basis attack against HFEv- is given by [13]

$$\mathrm{d_{reg}} \leq \begin{cases} \frac{(q-1)\cdot(r-1+a+v)}{2}+2 & q \text{ even and } r+a \text{ odd}, \\ \frac{(q-1)\cdot(r+a+v)}{2}+2 & \text{otherwise.} \end{cases}, \tag{11}$$

where r is given by $r = \lfloor \log_q(D-1) \rfloor + 1$.

[**35**] In [7] Courtois et al. estimated the complexity of a direct attack on QUARTZ by 2^{74} operations. However, they underestimated the degree of regularity of solving an HFEv- system drastically.

[**36**] Efficiency: The most costly step during the signature generation process of QUARTZ is the inversion of the univariate polynomial equation $\mathcal{F}_V$ over the extension field $\mathbb{E}$. This step is usually performed by Berlekamp's algorithm, whose complexity can be estimated by [26]

$$\mathcal{O}(D^3 + n \cdot D^2). \tag{12}$$

[**37**] Due to the high degree of the HFE polynomial used in QUARTZ, the inversion of $\mathcal{F}$ is very costly. Furthermore, we have to perform this step four times during the signature generation of QUARTZ. Additionally, the design of QUARTZ requires the central equation $\mathcal{F}(Y)-X = 0$ to have a unique root. Since, after choosing random values for Minus equations and Vinegar variables, $\mathcal{F}$ can be seen as a random function, this requires about e trials to obtain a signature. Thus, the QUARTZ signature scheme is rather slow and it takes about 11 seconds to generate a signature [4].

[**38**] The theoretical breakthrough mentioned above indicates that we can substantially improve the original design of QUARTZ without weakening the security of the scheme by reducing the degree D of the HFE polynomial in use, if we adapt the number of Minus equations and Vinegar variables in an appropriate way. By reducing the degree of the central HFE polynomial we can speed up the operations of Berlekamp's algorithm and therefore the signature generation process of the HFEv- scheme.

[**39**] We now present the new HFEv- design. The key question we need to answer is the following: How should we choose the degree D of the central HFE polynomial? A small D will speed up the scheme, but choosing D too small might bring the security of the scheme into jeopardy.

[**40**] With experiments and theoretical considerations, we determine that we should use $D \leq 33$. We determine that we should not use $D = 2$ ("Square" systems) or 3, since such small values of D would lead to maps $\mathcal{F}$ of rank 2. In order to find a balance between security and efficiency, we choose D to be 9 or 17.

[**41**] Since increasing a and v does not have a significant impact on the efficiency of the scheme, we determine that we should adjust a and v according to the security requirement and we propose that $a + v$ should be at least 8.

[**42**] Based on our experiments, to achieve a security level of 80 bits, we propose two different versions of our HFEv- based signature scheme over the field GF(2):

- Gui-95 with $(n, D, a, v) = (95, 9, 5, 5)$ with 90 equations in 100 variables and
- Gui-94 with $(n, D, a, v) = (94, 17, 4, 4)$ with 90 equations in 98 variables

[**43**] For a higher level of security, we propose Gui-127, with the parameters $(n, D, a, v) = (127, 9, 4, 6)$, providing a design security level of 120 bits.

[**44**] As in the case of QUARTZ, we have to repeat the inversion of the HFEv- core map several times to avoid birthday attacks against Gui. One has to sign different hash

values of the same message and combine the outputs into a single signature. Here, we follow the design of QUARTZ and apply the core HFEv- operation multiple times (4, 3 and 4 times respectively) for Gui-94, -95 and -127.

[45] These new Gui designs are much faster (hundreds of times) than the original QUARTZ scheme.

[46] One can also use a different $q \neq 2$. In this case, we determine that the degree of the HFE polynomial shall be $\leq q^5 + 1$.

1.2 The New White-box Encryption using Multivariate Digital Signatures

[47] We will now describe a new invention to perform white-box encryption when we have a practical multivariate public key signature scheme like what we described above.

[48] Cryptography is used to protect a communication channel. Normally in the design of cryptosystems, the end points are assumed to be secure and the attacker only has access to the input/output of the algorithm. In this case, the algorithm needs to be executed in a secure setting. However, for practical applications, the main problem are situations in which such a black-box security model does not apply any more. There have been a lot of new cryptanalysis techniques that incorporate additional side-channel information such as execution timing, electromagnetic radiation and power consumption to break the system. Currently, there has been proposed a more practical attack model [6], where cryptography is used on open devices anyone can access. This is called a white-box attack model, where an attacker has full access to the software implementation of a cryptographic algorithm and has full control over the execution platform. The key challenge here is to implement the cryptographic algorithm in software in such a way that cryptographic assets remain secure under white-box attacks. Such implementations play a key role in protecting digital assets, for example in Digital Rights Management (DRM) applications.

[49] The notion of white-box cryptography (WBC) has been introduced in [6]. The initial motivation was to embed symmetric secret keys into the implementation of popular standards like AES or DES in a way that binds the attacker to the specific implementation for DRM purposes. The main idea of this is to obfuscate key-dependent parts of the cipher and publish them as lookup tables. However, most of these constructions are not secure.

[50] To formalize the problem, two notions have been suggested for white-box encryption schemes. The goal of a weak white-box implementation of a cryptographic primitive is to prevent key-recovery attacks. This ensures that unauthorized users can not obtain any compact representation of the key which can be used to decrypt the protected content. The strong white-box implementation of a primitive prevents plaintext-recovery attacks.

[51] In [2] , Biryukov et al. proposed to use multivariate encryption schemes to construct white-box encryption schemes that not only hide the key for the weak white-box implementation, but also provide non-invertibility aiming for the strong white-box construction. However, their schemes have been broken.

[52] We propose here to use multivariate signature schemes to build a white box encryption scheme. Our technique is applicable to all existing multivariate signature schemes including HFEv- [24] and the improvements above. Here, we will use the example of Rainbow [12] to explain how our technique works.

[53] The Rainbow signature scheme [12] is one of the most promising and best studied multivariate signature schemes. The scheme is defined as follows: Let Let $\mathbb{F}$ be a finite field,

$n \in \mathbb{N}$ and $v_1 < v_2 < \cdots < v_\ell < v_{\ell+1} = n$ be a sequence of integers. We set $o_i = v_{i+1} - v_i$, $O_i = \{v_i + 1, \ldots, v_{i+1}\}$ and $V_i = \{1, \ldots, v_i\}$ $(i = 1, \ldots \ell)$. The number of elements in O_i is given by o_i and we have $|V_i| = v_i$ $(i = 1, \ldots, \ell)$.

[**54**] Key Generation: The *private key* consists of two invertible affine maps $\mathcal{S} : \mathbb{F}^m \to \mathbb{F}^m$ and $\mathcal{T} : \mathbb{F}^n \to \mathbb{F}^n$ and a quadratic map $\mathcal{F}(\mathbf{x}) = (f^{(v_1+1)}(\mathbf{x}), \ldots, f^{(n)}(\mathbf{x})) : \mathbb{F}^n \to \mathbb{F}^m$. Here, $m = n - v_1$ is the number of components of $\mathcal{F}$.
The components of the central map $\mathcal{F}$ are of the form

$$f^{(i)} = \sum_{k,l \in V_j} \alpha_{k,l}^{(i)} \cdot x_k \cdot x_l + \sum_{k \in V_j, l \in O_j} \beta_{k,l}^{(i)} \cdot x_k \cdot x_l + \sum_{k \in V_j \cup O_j} \gamma_k^{(i)} \cdot x_k + \eta^{(i)},$$

where j is the only integer such that $i \in O_j$.
The *public key* is the composed map $\mathcal{P}(\mathbf{x}) = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}(\mathbf{x}) : \mathbb{F}^n \to \mathbb{F}^m$.

[**55**] Signature Generation: To generate a signature for a document $\mathbf{h} \in \mathbb{F}^m$, we compute recursively $\mathbf{x} = \mathcal{S}^{-1}(\mathbf{h})$, $\mathbf{y} = \mathcal{F}^{-1}(\mathbf{x})$ and $\mathbf{z} = \mathcal{T}^{-1}(\mathbf{y})$. Here, $\mathcal{F}^{-1}(\mathbf{x})$ means finding one (of approximately q^{v_1}) pre-image of $\mathbf{x}$ under the central map $\mathcal{F}$. In the case of Rainbow, this is done as follows.

Algorithm 1 Inversion of the Rainbow central map

1: Choose random values for the variables $y_1, \ldots, y_{v_1}$ and substitute them into the polynomials $f^{(i)}$ $(i = v_1 + 1, \ldots n)$.
2: **for** $k = 1$ to ℓ **do**
3: Perform Gaussian Elimination on the polynomials $f^{(i)}$ $(i \in O_k)$ to get values for the variables y_i $(i \in O_k)$.
4: Substitute the values of y_i $(i \in O_k)$ into the polynomials $f^{(i)}$ $(i \in v_{k+1} + 1, \ldots n)$.
5: **end for**

It might happen that one of the linear systems in step 3 of the algorithm does not have a solution. In this case one has to choose other values for $y_1, \ldots, y_{v_1}$ and start again. The signature of the document $\mathbf{h}$ is $\mathbf{z} \in \mathbb{F}^n$.

[**56**] Signature Verification: To check the authenticity of a signature $\mathbf{z} \in \mathbb{F}^n$, one simply computes $\mathbf{h}' = P(\mathbf{z})$. If $\mathbf{h}' = \mathbf{h}$ holds, the signature is accepted, otherwise rejected.

[**57**] In the following, we will use Rainbow to demonstrate how to build a white-box encryption scheme using a multivariate signature scheme. However, our construction can be applied to any multivariate signature scheme including QUARTZ and Gui.

[**58**] In a practical scenario, a sender (e.g. TV company) broadcasts its program in the form of encrypted messages to a set $\mathcal{R}$ of receivers. The TV company is able to both en- and decrypt messages, whereas the receivers can only decrypt the sent messages. Unlegitimate users should not be able to decrypt the program, even with the help of a receiver $r \in \mathcal{R}$. Therefore, the receivers are not directly in the possession of the decryption key; instead of this, the key is embedded in a concrete implementation or a hardware device. To prevent the user from extracting the key out of the device, the key dependent parts of the cipher are hidden in a series of look-up tables. The main security requirements of our scenario are

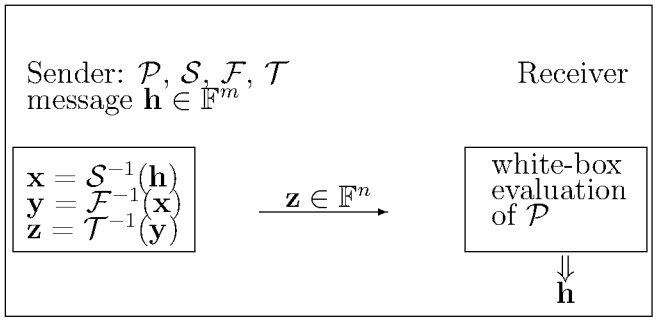


FIGURE 2. White-box implementation of a multivariate signature scheme

- **No key extraction**: It should be infeasible for the receivers to extract the public key from the device.
- **One-wayness**: A receiver can use his device only to decrypt messages from the sender; he can not encrypt his own messages.
- **Traceability**: When a receiver $r \in \mathcal{R}$ gives his device to an unlegitimate user, the identity of the receiver r can be revealed.

The security requirements "No key extraction" and "One-wayness" correspond closely to the notions of weak and strong white-box implementations of symmetric ciphers. However, instead of using a symmetric cipher such as AES or DES, we here look at public key, in particular multivariate schemes.

[**59**] Our technique to transform a multivariate signature scheme into a white-box encryption scheme can be described as follows.

[**60**] The sender (e.g. a TV-company) wants to broadcast a program to its receivers. Let $\mathcal{P}$ be the public key of a multivariate signature scheme such as Rainbow and ($\mathcal{S}$, $\mathcal{F}$, $\mathcal{T}$) be the corresponding private key. The sender is in possession of both the public and private key, whereas the receivers only have the public key (embedded in an hardware device).

[**61**] Encryption: To encrypt a message $\mathbf{h} \in \mathbb{F}^m$, the TV company computes recursively $\mathbf{x} = \mathcal{S}^{-1}(\mathbf{h})$, $\mathbf{y} = \mathcal{F}^{-1}(\mathbf{x})$ and $\mathbf{z} = \mathcal{T}^{-1}(\mathbf{y})$. Here, $\mathcal{F}^{-1}(\mathbf{x})$ means finding one (of possibly many) pre-image of $\mathbf{x}$ under the central map $\mathcal{F}$. In the case of Rainbow this is done as shown in Algorithm 1. The ciphertext of the message $\mathbf{h}$ is $\mathbf{z} \in \mathbb{F}^n$.

[**62**] **White-Box Decryption**: To decrypt the ciphertext $\mathbf{z} \in \mathbb{F}^n$, the hardware device simply evaluates the public key $\mathcal{P}$ at $\mathbf{z}$. As shown below (item 73 ff.), this can be easily done via look-up tables.

[**63**] The encryption process as described above consists of computing a signature $\mathbf{z} \in \mathbb{F}^n$ for the message $\mathbf{h} \in \mathbb{F}^m$. The white-box decryption corresponds widely to the verification process of the signature scheme (see Figure 2).

[**64**] In the setting of digital rights management, let us consider the example of a company selling e-books online. For each user, the company produces a specific key $\mathcal{P}_U$.

This $\mathcal{P}_U$ needs to be securely given to the user U and U is not allowed to give it to anyone else. If U hands his key to other users, the company can prove this, since $\mathcal{P}_U$ is a key uniquely belonging to U. The company can produce a software computing $\mathcal{P}_U$ or it can also use hardware technology to bind U to a hardware from which it is very costly to derive $\mathcal{P}_U$, or we can bind $\mathcal{P}_U$ to a specific hardware device, such that only designated devices can perform decryption using $\mathcal{P}_U$.

[**65**] When the company needs to send a book to the user U, it proceeds as follows. For each block $\mathbf{h} \in \mathbb{F}^m$ of the book file it uses, similar to the case of signature generation, the secret key attached to $\mathcal{P}_U$ to compute an encrypted version $\mathbf{z} \in \mathbb{F}^n$ of the block. The encrypted blocks are collected in a new file, which is then sent to the user U.

[**66**] The user can use his key $\mathcal{P}_U$ to decrypt each block in the encrypted file and then put the single blocks together in order to recover the original book file.

[**67**] In this setting, we produce a white-box encryption.

[**68**] In addition, due to the fact that we have a message expansion (for signature schemes we have $n > m$), we can use the extra information space to put more information inside which can be used it for further purposes.

[**69**] Due to the high efficiency of Rainbow, our system is much more efficient than those described in [2].

[**70**] We can also combine the decryption and reading function together in the hardware such that it is extremely costly to extract the pubic key from the hardware. This will serve well for the purpose of digital rights managements.

[**71**] We can also increase the key size of Rainbow by using smaller fields in order to make the system more secure in terms of public key extraction. This can be done in two different ways.

1) direct use of smaller fields and adjusting the parameters to a larger key size.

2) splitting the base field into smaller fields and adding random linear transformations $\mathcal{S}, T$ over the smaller field.

[**72**] In the implementation of decryption process of our white-box scheme, we propose a new idea of modified tables.

[**73**] The basic idea is as follows.

Addition and multiplication over the finite field F are essentially maps

$$F \times F \to F,$$

which can be implemented as look-up tables.

[**74**] In the case of multiplication, we have

$$x_i \times x_j = (ax_i) \times a^{(-1)}x_j$$

and

$$a_{ij}x_i \times x_j = (a_{ij}ax_i) \times a^{(-1)}x_j.$$

In the case of addition, we have

$$x_i + x_j = (a + x_i) + (-a + x_j)$$

and

$$b + x_i + x_j = (b + a + x_i) + (b - a + x_j).$$

Therefore, we have a large number of possibilities to modify the above look-up tables.

[75] In addition, we can use different irreducible polynomials to define the same finite fields or use field isomorphisms to modify the tables. By doing so, we obtain a large variety of possible table implementations.

[76] Even more generally, we can similarly use any randomly selected permutation map to modify the tables.

[77] We can use the modified tables to implement the whole decryption process using the public key map. This gives us an implementation to make the reverse engineering very costly.

[78] We can also compose two signature schemes together using composition of maps to build a degree 4 white-box encryption scheme. By using a small amount of internal perturbation, there is an efficient way to block the decomposition of such a map.

[79] The One-wayness of our implementation is guaranteed by the use of a public key signature scheme. To encrypt messages, a user has to know the private key of the signature scheme, which is only known by the sender. Therefore, the One-wayness of our scheme is guaranteed as long as the underlying signature scheme is secure.

References

[1] D.J. Bernstein, J. Buchmann, E. Dahmen (eds.): Post Quantum Cryptography. Springer, 2009.

[2] A. Biryukov, C. Bouillaguet, D. Khovratovich: Cryptographic Schemes Based on the ASASA Structure: Black-Box, White-Box, and Public-Key (Extended Abstract). ASIACRYPT (1) 2014: 63-84

[3] A. Bogdanov, T. Eisenbarth, A. Rupp, C. Wolf. Time-area optimized public-key engines: MQ-cryptosystems as replacement for elliptic curves? CHES 2008, LNCS vol. 5154, pp. 45-61. Springer, 2008.

[4] A.I.T. Chen, M.-S. Chen, T.-R. Chen, C.-M. Cheng, J. Ding, E. L.-H. Kuo, F. Y.-S. Lee, B.-Y. Yang. SSE implementation of multivariate PKCs on modern x86 cpus. CHES 2009, LNCS vol. 5747, pp. 33 - 48. Springer, 2009.

[5] S. Chow, P. Eisen, H. Johnson, P. C. van Oorschot. A white-box DES implementation for DRM applications. Digital Rights Management Workshop, LNCS vol. 2696, pages 1-15. Springer, 2002.

[6] S. Chow, P. Eisen, H. Johnson, P.C. van Oorschot: White-Box Cryptography and an AES Implementation. SAC 2002, LNCS vol. 2595, pp. 250 - 270. Springer 2003.

[7] N.T. Courtois, M. Daum, P. Felke: On the Security of HFE, HFEv- and QUARTZ. PKC 2003, LNCS vol. 2567, pp. 337 - 350. Springer 2003.

[8] J. Ding, J. E. Gower, D. S. Schmidt: Multivariate Public Key Cryptosystems. Springer, 2006.

[9] J. Ding, T. Hodges: Inverting HFE Systems Is Quasi-Polynomial for All Fields. CRYPTO 2011, LNCS vol. 6841, pp. 724-742. Springer 2011.

[10] J. Ding, T. Kleinjung: Degree of regularity for HFE-. IACR eprint 2011/570.

[11] J. Ding, A. Petzoldt, L.-C. Wang: The Cubic Simple Matrix Encryption Scheme. PQCrypto 2014, LNCS vol. 8772, pp. 76-87. Springer, 2014.

[12] J. Ding, D. S. Schmidt: Rainbow, a new multivariate polynomial signature scheme. ACNS 2005, LNCS vol. 3531, pp. 164-175. Springer, 2005.

[13] J. Ding, B.Y. Yang: Degree of Regularity for HFEv and HFEv-. PQCrypto 2013, LNCS vol. 7932, pp. 52-66. Springer, 2013.

[14] J.C. Faugère: A new efficient algorithm for computing Groebner bases (F4). Journal of Pure and Applied Algebra 139, pp. 61-88 (1999).

[15] J.C. Faugère, A. Joux: Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Groebner Bases. CRYPTO 2003, LNCS vol. 2729, pp. 44-60. Springer, 2003.

[16] M. R. Garey and D. S. Johnson: Computers and Intractability: A Guide to the Theory of NP-Completeness. W.H. Freeman and Company, 1979.

[17] A. Kipnis, L. Patarin, L. Goubin: Unbalanced Oil and Vinegar Schemes. EUROCRYPT 1999. LNCS vol. 1592, pp. 206-222 Springer, 1999.

[18] A. Kipnis, A. Shamir: Cryptanalysis of the HFE Public Key Cryptosystem. CRYPTO 99, LNCS vol. 1666, pp. 19 - 30. Springer, 1999.

[19] D. Kravitz: Digital Signature Algorithm. US Patent 5,231,668 (July 1991).

[20] T. Matsumoto, H. Imai: Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. EUROCRYPT 1988, LNCS vol. 330, pp. 419-453. Springer, 1988.

[21] M. S. E. Mohamed, J. Ding and J. Buchmann: Towards Algebraic Cryptanalysis of HFE Challenge 2, ISA 2011, Communications in Computer and Information Science vol. 200, pp. 123-131. Springer, 2011.

[22] J. Patarin: Cryptographic communication process. US Patent 5,790,675 (July 1996).

[23] J. Patarin: Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt 88. CRYPTO 95, LNCS vol. 963, pp. 248 - 261. Springer, 1995.

[24] J. Patarin, N. Courtois, L. Goubin: QUARTZ, 128-Bit Long Digital Signatures. CTRSA 2001, LNCS vol. 2020, pp. 282-297. Springer, 2001.

[25] J. Patarin, N. Courtois, L. Goubin: Flash, a fast multivariate signature algorithm. CTRSA 2001, LNCS vol. 2020, pp. 298 - 307. Springer, 2001.

[26] C. Richards: Algorithms for Factoring Square-Free Polynomials over Finite Fields. Master Thesis. Simon Fraser University (Canada), 2009.

[27] R. L. Rivest, A. Shamir, L. Adleman: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Commun. ACM 21 (2), pp. 120-126 (1978).

[28] P. Shor: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM J. Comput. 26 (5), pp. 1484 - 1509.
[29] C. Tao, A. Diene, S. Tang, J. Ding: Simple Matrix Scheme for Encryption. PQCrypto 2013, LNCS vol. 7932, pp. 231-242. Springer, 2013.

CLAIMS

[1] Claim 1. A Method for establishing an improved digital signature scheme, comprising:

A user establishes its public and private key in the following steps:

(1) *The user chooses a finite field* $\mathbb{F} = \mathbb{F}_q$ *with* q *elements and a degree* n *extension field* $\mathbb{E}$ *of* $\mathbb{F}$. *The user chooses integers* D, a *and* v. **The parameters are chosen in such a way that** $(\mathbb{F}, n, D, a, v) = (\mathrm{GF}(2), n, D, a, v)$ **,** $D \leq 33$ **and** $a+v \geq 8$**.**

Let Φ *be the canonical isomorphism between* $\mathbb{F}^n$ *and* $\mathbb{E}$, *i.e.*

$$\Phi(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i \cdot X^{i-1}.$$

(2) *The user chooses the central map* $\mathcal{F}$ *of the scheme as a map from* $\mathbb{E} \times \mathbb{F}^v$ *to* $\mathbb{E}$ *of the form*

$$\mathcal{F}(X) = \sum_{i,j=0}^{q^i+q^j \leq D} \alpha_{i,j} \cdot X^{q^i+q^j} + \sum_{i=1}^{q^i \leq D} \beta_i(v_1, \ldots, v_v) \cdot X^{q^i} + \gamma(v_1, \ldots, v_v),$$

with $\alpha_{i,j} \in \mathbb{E}$, $\beta_i : \mathbb{F}^v \to \mathbb{E}$ *being linear and* $\gamma : \mathbb{F}^v \to \mathbb{E}$ *being a quadratic function. Hereby, the coefficients* α_{ij} *as well as the coefficients of the maps* β_i *and* γ *are randomly selected elements of* $\mathbb{E}$.

(3) *The user builds its public key as the composed map* $\mathcal{P} = \mathcal{S} \circ \bar{\mathcal{F}} \circ \mathcal{T} : \mathbb{F}^{n+v} \to \mathbb{F}^{n-a}$, *where* $\bar{\mathcal{F}} = \Phi^{-1} \circ \mathcal{F} \circ \Phi$ *and* $\mathcal{S} : \mathbb{F}^n \to \mathbb{F}^{n-a}$ *and* $\mathcal{T} : \mathbb{F}^{n+v} \to \mathbb{F}^{n+v}$ *are randomly selected affine linear maps of maximal rank. The private key consists of* $\mathcal{S}$, $\mathcal{F}$ *and* $\mathcal{T}$. *This public key is a set of quadratic polynomials.*

A signature for a message $\mathbf{h} \in \mathbb{F}^{n-a}$ *is computed as follows:*

(1) *Compute a pre-image* $\mathbf{x} \in \mathbb{F}^n$ *of* $\mathbf{h}$ *under the affine map* $\mathcal{S}$.

(2) *Lift* $\mathbf{x}$ *to the extension field* $\mathbb{E}$ *(using the isomorphism* Φ*). Denote the result by* X.
Choose random values for the Vinegar variables $v_1, \ldots, v_v \in \mathbb{F}$ *and compute* $\mathcal{F}_V = \mathcal{F}(v_1, \ldots, v_v)$.
Solve the univariate polynomial equation $\mathcal{F}_V(Y) = X$ *by Berlekamp's algorithm and compute* $\mathbf{y}' = \Phi^{-1}(Y) \in \mathbb{F}^n$.
Set $\mathbf{y} = (\mathbf{y}' || v_1 || \ldots || v_v)$.

(3) *Compute the signature* $\mathbf{z} \in \mathbb{F}^{n+v}$ *by* $\mathbf{z} = \mathcal{T}^{-1}(\mathbf{y})$.

Anyone can verify the authenticity of a signature $\mathbf{z} \in \mathbb{F}^{n+v}$ *by simply computing* $\mathbf{h}' = \mathcal{P}(\mathbf{z}) \in \mathbb{F}^{n-a}$. *If* $\mathbf{h}' = \mathbf{h}$ *holds, the signature is accepted, otherwise rejected.*

[2] Claim 2. A scheme according to Claim 1 obtained by choosing a different prime q, $D \leq q^5 + 1$ *and* $a + v \geq 8$.

[3] Claim 3. A scheme according to Claim 1, for which the length of signature is short (less than 128 bits), the user signs the message $\mathbf{h}$ *and the hash of its padded values multiple*

(≤ 3) times and combines the single signatures to a single long signature of the message $\mathbf{h}$. *During the signature verification process, the public key* $\mathcal{P}$ *is used the same number of times.*

[4] Claim 4. A method to build a white-box encryption scheme using a multivariate signature scheme, comprising:

- *A user who broadcasts information, e.g. a TV company. First, the user chooses a multivariate signature scheme as follows:*
  (1) *the user starts with an easily invertible quadratic map* $\mathcal{F} : \mathbb{F}^n \to \mathbb{F}^m$ *(central map). Then the user composes* $\mathcal{F}$ *with two randomly selected invertible affine (or linear) maps* $\mathcal{S} : \mathbb{F}^m \to \mathbb{F}^m$ *and* $\mathcal{T} : \mathbb{F}^n \to \mathbb{F}^n$. *The public key is the composed map* $\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}$. *The private key consists of* $\mathcal{S}$, $\mathcal{F}$ *and* $\mathcal{T}$ *and allows the user to invert the public key. Here we have* $n \geq m$.
  (2) *this signature system comprises two processing components:*

  Signature generation: To sign a message $\mathbf{h} \in \mathbb{F}^m$, *the user computes recursively* $\mathbf{x} = \mathcal{S}^{-1}(\mathbf{h}) \in \mathbb{F}^n$, $\mathbf{y} = \mathcal{F}^{-1}(\mathbf{x}) \in \mathbb{F}^n$ *and* $\mathbf{z} = \mathcal{T}^{-1}(\mathbf{y})$. *Here,* $\mathcal{F}^{-1}(\mathbf{x})$ *means finding one (of possibly many) pre-image of* $\mathbf{x}$ *under the central map* $\mathcal{F}$. *The signature of the message* $\mathbf{h}$ *is* $\mathbf{z} \in \mathbb{F}^n$.

  Verification: To check the authenticity of a signature $\mathbf{z} \in \mathbb{F}^n$, *one simply computes* $\mathbf{h}' = \mathcal{P}(\mathbf{z}) \in \mathbb{F}^n$. *If* $\mathbf{h}' = \mathbf{h}$ *holds, the signature is accepted, otherwise rejected.*
- *The user (e.g. a TV-company), who broadcasts a program to its receivers, implements the evaluation of the selected public key* $\mathcal{P}$ *in a hardware device in such a way that it is very difficult and very costly to extract the public key from the device.*
- *To encrypt a message* $\mathbf{h} \in \mathbb{F}^m$, *the user (the TV company) just performs the signature generation algorithm of the multivariate signature scheme to compute the ciphertext* $\mathbf{z} \in \mathbb{F}^n$ *of the message* $\mathbf{h}$.
- **White-Box Decryption***: To decrypt the ciphertext* $\mathbf{z} \in \mathbb{F}^n$, *the hardware device simply evaluates the public key* $\mathcal{P}$ *at* $\mathbf{z}$.

[5] Claim 5. A method according to Claim 4, where the evaluation of the public key $\mathcal{P}$ *is performed in a hardware device by multiplication and addition of* $\mathbb{F}$*-elements using different lookup tables.*

[6] Claim 6. A method according to Claim 4, where each receiver U *is given a specific key* $\mathcal{P}_U$. *This* $\mathcal{P}_U$ *needs to be securely transmitted to the receiver* U. U *is not allowed to give his key to anyone else, and if* U *does, the user can prove this using the fact that* P_U *belongs uniquely to the receiver* U.

[7] Claim 7. A method according to Claim 4, where the user produces a software computing $\mathcal{P}_U$ *from which it is very costly to derive* $\mathcal{P}_U$ *and only designated hardware devices can perform decryption using* $\mathcal{P}_U$.

[8] Claim 8. A method according to Claim 4, where the user uses the extra information space provided by the fact that, in our signature scheme, we have $n > m$, *to put more information inside which can be used for further purposes such as tracing the receivers or detecting illegitimate copies, counting the number of decryptions etc.*

[9] Claim 9. A method according to Claim 4, where the user combines the decryption and the function of reading or playing a movie or any application of the data for usage

together in the hardware device such that it is very costly to intercept the decrypted raw data or to get the pubic key from the hardware.

[10] Claim 10. A method according to Claim 4, where the user also increases the key size of the signature scheme by using smaller fields to make the system more secure in terms of public key extraction in the following ways.

1) use of smaller fields and adjusting the parameters to a larger key size.

2) splitting up the base field into smaller fields and use of additional random linear transformations $\mathcal{S}, T$ on the smaller field.

3) increasing the parameters including the field size, extension field size etc.

[11] Claim 11. A method according to Claim 5, where the user can modify the tables using the following algebraic methods:

Addition and multiplication over a finite field F is essentially a map

$$F \times F \to F,$$

which can be implemented as a look-up table. The tables itself can be modified as follows.

- *In the case of multiplication, we have*

$$x_i \times x_j = (ax_i) \times a^{(-1)}x_j$$

and

$$a_{ij}x_i \times x_j = (a_{ij}ax_i) \times a^{(-1)}x_j.$$

- *In the case of addition, we have*

$$x_i + x_j = (a + x_i) + (-a + x_j)$$

and

$$b + x_i + x_j = (b + a + x_i) + (b - a + x_j).$$

The user can randomly select a in order to modify the tables.

[12] Claim 12. A method according to Claim 5, where the user uses different irreducible polynomials to define the same finite fields in different ways and/or uses field isomorphisms to modify the tables.

[13] Claim 13. A method according to Claim 5, where the user uses any randomly selected permutation map over the small field to modify the tables.

[14] Claim 14. A method according to Claim 4, where the user composes two signature schemes together using composition of maps to build a degree 4 white-box encryption, and /or uses internal perturbation in order to block the decomposition of such a map.

[15] Claim 15. A method according to Claim 4, where the user directly uses higher degree (3 or 4) signature schemes for white-box encryption.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/077293

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS;CNTXT;CNKI;VEN;IEEE;ACM;NIST: multivariate, digital, signature, quartz, hfe, hfev, hidden, field, equation?, white?box,

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 102006168 A (UNIV XIAN TECHNOLOGY) 06 April 2011 (2011-04-06) The whole document	1-15
A	US 2014380062 A1 (SONY CORP) 25 December 2014 (2014-12-25) The whole document	1-15
PX	Jintai Ding et al. "Gui:Revisitiong Multivariate Digtal Signature Schemes based on HFEv-" *csrc.nist.gov/groups/ST/post-quantum-2015/presentations/session1-ding-jintai.pdf,* 09 April 2015 (2015-04-09), Pages 2-30	1-15

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 May 2016	**12 June 2016**
Name and mailing address of the ISA/CN **STATE INTELLECTUAL PROPERTY OFFICE OF THE P.R.CHINA** **6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing 100088, China** Facsimile No. **(86-10)62019451**	Authorized officer **LIU,Lin** Telephone No. **(86-10)62411953**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/077293

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 102006168 A	06 April 2011	CN 102006168 B	13 March 2013
US 2014380062 A1	25 December 2014	EP 2822218 A1	07 January 2015
		WO 2013129119 A1	06 September 2013