A New Perturbation for Multivariate Public Key Schemes such as HFE and UOV

Jean-Charles Faugère[4], Gilles Macario-Rat[1], Jacques Patarin[2,3], and Ludovic Perret[4]

[1] Orange, 46, avenue de la République, 92320 Châtillon, France
[2] UVSQ, CNRS, University of Paris-Saclay, France
[3] Thales DIS France SAS, 6, rue de la Verrerie, 92190 Meudon, France
[4] Cryptonext Security, 4, place Jussieu, Paris 75005, France
gilles.macariorat@orange.com jpatarin@club-internet.fr
{ludovic.perret,jcf}@cryptonext-security.com

Abstract. We present here the analysis of a new perturbation noted $\hat{+}$, that seems to strengthen significantly the security of some families of multivariate schemes. Thanks to this new perturbation, we are indeed able to get interestingly efficient signature and encryption public key schemes, in particular when combining this perturbation to the well known trapdoors HFE ([12]) and UOV ([9]). We present here the best attacks that we know against these variant schemes $\mathrm{HFE}^{\hat{+}\,-}$ and $\mathrm{UOV}^{\hat{+}}$ and we give practical examples of parameters for current standard of security.

Keywords: public-key cryptography, post-quantum multivariate cryptography, UOV, HFE, Gröbner basis, MinRank problem, differential attacks.

1 Introduction

Multivariate cryptography has interesting features for signature and encryption public key schemes. For example, the size of the signature can be very short. Currently, multivariate equations is one of the six large families of known techniques of post-quantum public key cryptography. The five other families are: hash based, isogenies, codes, lattices and combinatorial. However, multivariate cryptography is still under construction, many variants have been proposed but also many attacks still undermine their security, let's cite for instance famous schemes C*, SFLASH, GeMSS, Rainbow, and famous attacks, involving the differential, and the Minrank problem. In this article, we suggest new ideas that might repair or strengthen the security of multivariate schemes.

2 Notations and context

As in all classical multivariate schemes, we use a finite field $\mathbb{F}_q$ with q elements and we deal with the ring of polynomials in n variables $x_1, \ldots, x_n$ over $\mathbb{F}_q$, noted $\mathbb{F}_q[x_1,\ldots,x_n]$ (implicitly modulo $\langle x_1^q - x_1,\ldots,x_n^q - x_n\rangle$). Therefore here $\mathbb{F}_q[x_1,\ldots,x_n]^m$ will refer to the algebra of n-ary m-dimensional polynomials, that we call (n,m)-polynomials for short. We note $\Phi_m : \mathbb{F}_{q^m} \to \mathbb{F}_q^m$ the natural isomorphism mapping the field extension to its vector space (relatively to some $\mathbb{F}_q$-basis). For $\alpha \in \mathbb{F}_{q^m}$, we denote $\bar{\alpha} = \Phi_m(\alpha)$, $\bar{\alpha} \in \mathbb{F}_q^m$. By extension and as a shorthand, we denote $\bar{x} = (x_1,\ldots,x_m)$. We denote φ the Frobenius mapping $\varphi : \mathbb{F}_{q^m} \mapsto \mathbb{F}_{q^m},\ x \to x^q$; the multipliers mappings Λ_α, $\alpha \in \mathbb{F}_{q^m}$ are $\Lambda_\alpha : \mathbb{F}_{q^m} \mapsto \mathbb{F}_{q^m},\ x \to \alpha x$; and finally the well known linear mapping "trace" is $\mathrm{Tr}_m : \mathbb{F}_{q^m} \mapsto \mathbb{F}_q,\ x \to \sum_{i=0}^{m-1} x^{q^i}$. For consistency, computations over $\mathbb{F}_{q^m}[x]$ are also implicitly done modulo $\langle x^{q^m} - x\rangle$.

To deal with different dimensions, we define a natural embedding :

$$I_{m,n} : \mathbb{F}_q^m \mapsto \mathbb{F}_q^n, (x_1,\ldots,x_m) \to \begin{cases} (x_1,\ldots,x_n) & \text{when } n \leq m, \\ (x_1,\ldots,x_m,\overbrace{0,\ldots,0}^{n-m}) & \text{when } n > m. \end{cases}$$

For a univariate polynomial F of $\mathbb{F}_{q^n}[x]$, we denote $\hat{F} = \Phi_n \circ F \circ \Phi_n^{-1}$ where $\hat{F} : \mathbb{F}_q^n \mapsto \mathbb{F}_q^n$, that is $\hat{F}$ is a (n,n)-polynomial. For instance, the Frobenius φ is a linear polynomial of degree q of $\mathbb{F}_{q^n}[x]$, whereas $\hat{\varphi}$ is a linear (n,n)-polynomial of degree 1 of $\mathbb{F}_q[\bar{x}]^n$. Note that we have trivially $\hat{x} = (x_1,\ldots,x_n)$.

Reciprocally, for P a (n,m)-polynomial $(n \geq m)$, we denote $\check{P} = \Phi_n^{-1} \circ I_{m,n} \circ P \circ \Phi_n$ where $\check{P}$ is a univariate polynomial of $\mathbb{F}_{q^n}[x]$.

We denote $\deg(P)$ the degree of a $(n,1)$-polynomial P. By extension, the degree of a (n,m)-polynomial is the maximum degree of its $(n,1)$-components.

We use $\mathcal{M}_{n,m}(\mathbb{F}_q)$ to denote the set of square $n \times m$-matrices with coefficients in $\mathbb{F}_q$, and we use the dot "." to denote the (row) vector-matrix product or the matrix-(column) vector. If v is a (row) vector, then u^{t} is its transposed (column) vector.

We call λ the security level, typically $\lambda = 128$. A scheme having a security level λ means that an attacker can not break it by performing less than 2^λ operations.

Computer experiments evoked in this paper, related to Gröbner basis have been performed on the on-line site of MAGMA `http://magma.maths.usyd.edu.au/calc/` [4]. Time measurement were performed on an Intel Core i7-6700 CPU, 3.4GHz, with a C++ program developed under Microsoft Visual Studio 2019.

3 Hat Plus $\hat{+}$: a new perturbation

3.1 The HFE$^{\hat{+}-}$ trapdoor

We first present the new perturbation $\hat{+}$ in the context of HFE, for which we recall the details. HFE uses a (so-called small) field $\mathbb{F}_q$ and one of its (so-called big) finite extension $\mathbb{F}_{q^n}$. Here q will be therefore a small power of 2 or a small odd prime or odd prime power, typically $q = 2$ or 64 or 59. Typical values of the degree of extension n will be such that q^n is approximately between 2^{λ} and $2^{2\lambda}$. The main component of the scheme HFE is a univariate polynomial which degree is bounded by d, another parameter of the scheme :

$$H(x) = \sum_{q^i+q^j \leq d} \alpha_{i,j} x^{q^i+q^j}.$$

For instance, $d = 1 + q^{\epsilon}$ is the smallest possible value (where $\epsilon = 1$ if q is even, and $\epsilon = 0$ if q is odd), but still larger degrees can be considered. Typical values of d are less than 1000 for instance.

The scheme is called HFE$^{\hat{+}\,-}$, which means there are two more parameters tuning the scheme : t, the dimension of the new perturbation called "Hat Plus", whose principles will be explained hereafter, and a, the "Minus" parameter. Typical values of these parameters will be such that a and t are smaller than n, and dq^t is quite small (less than 1000 for instance.)

We introduce now our new perturbation $\hat{+}$ [5], depending on t randomly chosen quadratic forms : $p_i(x_1, \ldots, x_n)$, $i = 1, \ldots, t$, (p_i are random homogeneous degree-2 $(n, 1)$-polynomial of $\mathbb{F}_q[\bar{x}]$), and t randomly chosen elements of $\mathbb{F}_{q^n}$: β_i, $i = 1, \ldots, t$. The perturbation is then simply :

$$Q(x) = \sum_{i=1,\ldots,t} \beta_i \check{p}_i(x).$$

We can express $p_i(x_1, \ldots, x_n) = \sum_{j,k} a_{i,j,k} x_j x_k$, but also viewed as a polynomial of $\mathbb{F}_{q^n}[x]$: $\check{p}_i(x) = \mathrm{Tr}_n(\sum_{j,k} \alpha_{i,j,k} x^{q^{j+k}})$. In the first expression $\{a_{i,j,k}\}$ are random elements of $\mathbb{F}_q$, and in the second one, $\{\alpha_{i,j,k}\}$ are random elements of $\mathbb{F}_{q^n}$ ($\{a_{i,j,k}\}$ and $\{\alpha_{i,j,k}\}$ deduce from each other). The latter expression shows that the degree of $\check{p}_i$ and hence also Q, is not bounded by a small value, but can be as big as $2q^{n-1}$, contrary to the trapdoor functions of HFE.

Then, we define $F = H + Q$ as the secret trapdoor. Using the "Minus" perturbation driven by the last parameter a, we select at random two additional linear secret mappings $S : \mathbb{F}_q^n \mapsto \mathbb{F}_q^{n-a}$ and $T : \mathbb{F}_q^n \mapsto \mathbb{F}_q^n$ (supposedly of maximum rank). Finally, we publish the public key of our HFE$^{\hat{+}\,-}$ scheme :

$$\mathcal{P} = S \circ \hat{F} \circ T,$$

which therefore will be a degree-2 homogeneous $(n, n-a)$-polynomial. The parameters q, n, d, t, and a being also public, the secret key consists in the description (coefficients in $\mathbb{F}_q$ or $\mathbb{F}_{q^n}$) of S, T, H and Q.

3.2 Special inversion of the HFE$^{\hat{+}}$ trapdoor

The special shape of the $\hat{+}$ perturbation was chosen such that it is of course possible to efficiently inverse the resulting trapdoor, that is to efficiently and

[5] This perturbation is very close to the + introduced by Patarin et al. in [13], however this is not exactly the same, hence the notation $\hat{+}$.

practically compute the solutions in x of the equation $F(x) = H(x) + Q(x) = y$, for any given y in $\mathbb{F}_{q^n}$. Since the degree of F (and Q) is huge (possibly $2q^{n-1}$), a direct method such as the Berlekamp algorithm cannot be used primarily. On the other hand, we can exploit the property that $\check{p}_i(x)$ is in $\mathbb{F}_q$. So it is possible to make an exhaustive search of the value of each $\check{p}_i(x)$ and in turn $Q(x)$ which therefore can take only q^t possibilities. A first method to solve $F(x) = y$ is to solve the q^t equations $H(x) = y - \sum_i r_i \beta_i$, $r_i \in \mathbb{F}_q$, (which can be solved using Berlekamp algorithm, since its degree is bounded by d), and to keep the solutions satisfying $\check{p}_i(x) = r_i$. A second method involves the elimination of Q by using the projection Π_t. Indeed we get $\Pi_t(F(x)) = \Pi_t(H(x)) = \Pi_t(y)$ which can be also solved using Berlekamp algorithm since the degree is bounded by dq^t. It suffices then to verify which solutions of this latter equation satisfy also $F(x) = y$. Theory shows that solving q^t degree-d polynomials (first method) is as much complex than solving one degree-dq^t polynomial (second method) (at least in asymptotic complexity). However by experimentation, it seems that when d is smaller, the first method is more efficient.

We also assume and have verified by experiments that the equation $F(x) = y$ behave almost as a random univariate equation over $\mathbb{F}_{q^n}$. Indeed, the probabilities that the equation has zero solution and one solution are very close to the theoretical value $\exp(-1)$; it has in average approximately one solution, like a random equation.

3.3 The UOV$^{\hat{+}}$ trapdoor

We present now the perturbation $\hat{+}$ in the context of UOV, for which we recall here the details. Computations are performed in a finite field $\mathbb{F}_q$. Two parameters h and v denote respectively the number of "oil" and "vingear" variables. Then, x_i, $i = 1, \ldots, h$ are called the oil variables, and x'_i, $i = 1, \ldots, v$ are called the vinegar variables. In this section for simplicity, x will denote $(x_1, \ldots, x_h)$, and so on for x', y, z, etc. The original secret trapdoor of UOV is a set of h quadratic polynomials in all variables, without "oil×oil" monomials :

$$\begin{aligned} y_1 &= \sum_{1 \le i \le j \le v} a_{1ij} x'_i x'_j + \sum_{\substack{1 \le i \le h \\ 1 \le j \le v}} b_{1ij} x_i x'_j, \\ &\vdots \\ y_h &= \sum_{1 \le i \le j \le v} a_{hij} x'_i x'_j + \sum_{\substack{1 \le i \le h \\ 1 \le j \le v}} b_{hij} x_i x'_j. \end{aligned}$$

We can define for short, $y = U(x, x')$, where U is a degree-2 homogeneous $(h + v, h)$-polynomial, degree-1 in the first h variables. The $\hat{+}$ perturbation is as previously composed by a set of t quadratic forms, in this case in oil variables :

$$
\begin{aligned}
z_1 &= \sum_{1 \le i \le j \le h} c_{1ij} x_i x_j, \\
&\vdots \\
z_t &= \sum_{1 \le i \le j \le h} c_{tij} x_i x_j.
\end{aligned}
$$

We define for short $z = Q(x)$, where Q is a degree-2 homogeneous (h, t)-polynomial. Then the secret $\mathrm{UOV}^{\hat{+}}$ trapdoor is the sum of the original trapdoor and linear combinations of the previous quadratic forms :

$$
\begin{aligned}
y'_1 &= \sum_{1 \le i \le j \le v} a_{1ij} x'_i x'_j + \sum_{\substack{1 \le i \le h \\ 1 \le j \le v}} b_{1ij} x_i x'_j + \sum_{1 \le i \le t} \lambda_{1i} z_i, \\
&\vdots \\
y'_h &= \sum_{1 \le i \le j \le v} a_{hij} x'_i x'_j + \sum_{\substack{1 \le i \le h \\ 1 \le j \le v}} b_{hij} x_i x'_j + \sum_{1 \le i \le t} \lambda_{hi} z_i.
\end{aligned}
$$

For short : $F(x, x') = U(x, x') + \Lambda(Q(x))$, where Λ is a degree-1 homogeneous (t, h)-polynomial. The coefficients a_{ijk}, b_{ijk}, c_{ijk}, and λ_{ij} are of course random elements of $\mathbb{F}_q$. We select at random two additional linear secret bijections $S : \mathbb{F}_q^h \mapsto \mathbb{F}_q^h$ and $T : \mathbb{F}_q^{h+v} \mapsto \mathbb{F}_q^{h+v}$. Finally, we publish

$$
\mathcal{P} = S \circ F \circ T,
$$

which therefore will be a degree-2 homogeneous $(h + v, h)$-polynomial. The parameters q, h, v, and t being public, the secret key consists in the description (coefficients in $\mathbb{F}_q$) of S, T, U, Q and Λ.

Remark 1. Since Λ can be supposed of maximum rank, it is always possible to have another secret decomposition with same public key, for which $\Lambda = I_{t,h}$ (canonical form of a $h \times t$ matrix of rank t).

3.4 Special inversion of the $\mathrm{UOV}^{\hat{+}}$ trapdoor

We explain here how to find solutions in (x, x') of the equation $F(x, x') = y$. As with the original UOV, a first step consists in selecting at random a vinegar value $x' = v$, then finding a solution in x of $F(x, v) = y$. For a second step and as in the previous case with HFE, use the exhaustive search of the q^t values of z. We are then brought back to solve q^t linear systems and check individually if one of its solutions is consistent with the $\hat{+}$ equation $Q(x) = z$. However there is an even better way than the exhaustive search. Consider the system $F(x, v) = y$ where the t forms of $Q(x)$ are replaced by new variables $z_1, \ldots, z_t$. We get then a linear system of h equations in $h + t$ variables. When the system has maximum rank, we can express the h oil variables as linear combinations of these new variables. We then replace the expression of the oil variables in the equations $Q(x) = z$ and get a quadratic system of t equations in t variables. This method can easily be adapted when the system has a rank default by adjusting accordingly the number of free variables. When the linear system has a rank default and is inconsistent, or when the deduced quadratic system has no solutions, just try a new value v for x' and redo the work.

4 Security analysis of HFE$^{\hat{+}-}$

For a convenient notation, we introduce here $r = \lfloor \log_q(d-1) \rfloor + 1$ known as the "rank" of the HFE polynomial. Rationale : when interpreting $H(x)$ as a quadratic form in $(x, x^q, \ldots, q^{n-1})$, then this form has at most rank r.

We note ω the linear algebra constant.

4.1 Perturbations and projections

Regarding the Minus perturbation, it has been noticed (see [15]) that it can be reinterpreted as the effect of a projection. Namely, for a given map $S : \mathbb{F}_q^n \mapsto \mathbb{F}_q^{n-a}$ (of rank $n - a$), we can find a bijective extension of S : $S^+ : \mathbb{F}_q^n \mapsto \mathbb{F}_q^n$ and a linear polynomial L_a of degree q^a and rank $n - a$ such that $S = S^+ \circ L_a$. Concerning the $\hat{+}$ perturbation, since obviously its image is the subspace spanned by the family $\{\beta_i\}$, that we can suppose of dimension t, we can find a linear polynomial $\mathit{\Pi}_t$ of degree q^t and rank t such that $\mathit{\Pi}_t \circ Q = 0$.

4.2 Equivalent keys

The study of equivalent keys is important to assess the security of a multivariate scheme (see [10]). In our case, two tuples of secret keys (S, T, F) and (S', T', F') are said equivalent if they lead to the same public key. A first step in this study is to determine the "sustainders", which are the families of linear mappings (σ, τ), such that $\sigma \circ F \circ \tau$ keeps the shame "shape". In other words, if F and $\sigma \circ F \circ \tau$ are admissible functions for the scheme, then (S, T, F) and $(S \circ \hat{\sigma}^{-1}, \hat{\tau}^{-1} \circ T, \sigma \circ F \circ \tau)$ are obviously equivalent keys.

Notice for instance that whatever the linear mapping τ, then $Q' = Q \circ \hat{\tau}$ is eligible for the Onyx scheme. Likewise, if H is a unitary HFE polynomial, then $H \circ \mathit{\Lambda}_\delta = \delta^d H'$, where H' is another eligible unitary HFE polynomial.

More generally, among the sustainders are the multipliers: $\mathit{\Lambda}_\gamma$, $\gamma \in \mathbb{F}_{q^n}$ and the iterates of the Frobenius: $\varphi^{(i)} : x \to x^{q^i}$. In particular, we have: $\mathit{\Lambda}_\gamma \circ (H + Q) \circ \mathit{\Lambda}_\delta = \lambda \delta^d H' + \lambda Q'$. So we see that it is always possible to find unitary H' and Q' that lead to an equivalent key. So from now, we may consider that H and Q are unitary. With this extra condition, the equivalent keys are most probably only the ones induced by the iterated Frobenius $(\sigma, \tau) = (\varphi^{(i)}, \varphi^{(n-i)})$, and the ones induced by the "small" multipliers $(\sigma, \tau) = (\mathit{\Lambda}_{1/a^2}, \mathit{\Lambda}_a)$, $a \in \mathbb{F}_q,\ a \neq 0$.

4.3 Weak keys

Following the example of [5], we should also be careful about undesired properties of F leading to structural attacks. We have just seen the existence of mappings (σ, τ), such that $\sigma \circ F \circ \tau$ is (part of) an equivalent key. However, is it possible to find (σ, τ) such that exactly $\sigma \circ F \circ \tau = F$? Indeed, this would lead to the following attack: find two linear mappings A and B such that $\mathcal{P} \circ A = B \circ \mathcal{P}$, then we would have something like : $A = T^{-1} \circ \hat{\tau}^{-1} \circ T$, and something similar for B (since S is not invertible). We know that the small field multipliers are such candidates, however they lead to trivial equations that reveal nothing about S and T. If we look at the Frobenius and its iterates, then a choice of p_i satisfying for all $x \in \mathbb{F}_q^n$, $p_i \circ \hat{\varphi}(\bar{x}) = p_i(\bar{x})$ (this is the case for instance if $p_i(\bar{x}) = \mathrm{Tr}(x^{1+q^i})$) leads indeed to a weak key. Since p_i may be chosen at random, it is very unlikely that this condition be fulfilled.

4.4 Rank of the HFE$^{\hat{+}}$ trapdoor

An important aspect of the HFE$^{\hat{+}}$ trapdoor is its rank, since any rank defect in the public key due to the secret function could be exploited by an attacker. Classically, the rank of a degree-2 polynomial P is the minimum number r of products of two linear polynomials L_{ij}, $j = 1, 2$, in the possible sums $P(x) = \sum_{i=1}^{r} L_{i1}(x)L_{i2}(x)$. Since the p_i are randomly chosen, we may assume that with overwhelming probability that Q and therefore also F have rank n.

4.5 Direct attacks

We would like to address here the issue of the algebraic attacks that aim to invert directly the system $\mathcal{P}(x) = y$. As far as techniques involving Gröbner basis computation are the best to solve this problem, we refer to [7] and estimate the well-known degree of regularity of the system to invert. Inversion of the secret central map F suggests it is related to the polynomial $\Pi_t \circ L_a \circ H$, whose rank is $r + t + a$. Therefore we conjecture that the degree of regularity of an Onyx system is

$$D_{\mathrm{reg}} = \frac{(q-1)(r+a+t-\epsilon)}{2}.$$

4.6 Rank attacks

The idea in [16] and all related Minrank attacks, is to exploit a rank default and turn it into a search of a linear combination of matrices having a small rank. In our case, starting from the equivalent form $\mathcal{P} = S^{+} \circ L_a \circ F \circ T$, we search an unknown mapping M such that either $M \circ \mathcal{P}$ (such as in [2]) or $\mathcal{P} \circ M$ (such as in [16]) has a rank default. For instance, following the lead of [2], we have $\Pi_t \circ (S^{+})^{-1} \circ \mathcal{P} = \Pi_t \circ L_a \circ H \circ T$, which has a small rank, namely $r + a + t$. The complexity of the corresponding attack using "Mirror Modelling" is therefore

$$O\left(\binom{n+r+a+t+1}{r+a+t+1}^{\omega}\right).$$

Following [16], we can observe [6] that each public equation $\mathcal{P}_i$ (or its matrix version) can be split into two parts, one deriving from a pure HFE H_i, and one from the $\hat{+}$ part Q_i. In [16], it has been shown that there exist vectors u such that the space vector $\langle uH_1, \ldots, uH_{n-a}\rangle$ has dimension at most r. Moreover for such vector u, $\langle uQ_1, \ldots, uQ_{n-a}\rangle$ has at most dimension t, due to the construction of the perturbation. Therefore $\langle u\,\mathcal{P}_1, \ldots, u\,\mathcal{P}_{n-a}\rangle$ has at most dimension $r+t$. We conclude that the corresponding attack should have at most complexity:

$$O\left(\binom{n+r+t+1}{r+t+1}^{\omega}\right).$$

even if we have not estimated the extra complexity required to complete the key recovery.

We analyse now a different way for an attacker to neutralize the effect of the $\hat{+}$ perturbation and how we should choose the parameters in consequence. We have already noticed that the public key can be expressed as $S^{+} \circ L_a \circ (H+Q) \circ T$. It means that multiplying the public key by the correct mapping $S^{+} \circ \Pi_t \circ (S^{+})^{-1}$, one could get $S^{+} \circ \Pi_t \circ L_a \circ H \circ T$. In other words, there exist (unknown) linear combinations of the public equations that can be interpreted as the public key of a HFE^{-} system with parameters $(q, n, r, t+a)$. So, suppose that we draw at random m linear combinations of the public equations, then with probability $1/q^{tm}$, they form a HFE^{-} public system with parameters $(q, n, r, n-m)$. Let's note $C_{-}(q, n, r, a)$ the cost of retrieving the key of a generic HFE^{-} system, then the overall cost of this attack is $q^{tm}C_{-}(q, n, r, n-m)$. We can estimate $C_{-}(q, n, r, a) = O\big(n^{\omega}\binom{2r+1}{r}^{\omega}\big)$, using the formula for support minors modeling in [1] (even better than the one in [16]). This formula does not depend of the number of removed equations, however this latter must be not too big: we must have $a < n - 2r - 1$. So in our case, we can estimate that the complexity of the attack is at least

$$q^{(2r+1)t}\left(n^{\omega}\binom{2r+1}{r}^{\omega}\right).$$

This leads to potential sets of parameters of n, r, and t that make us safe from this attack.

5 Security analysis of UOV$^{\hat{+}}$

5.1 Direct attacks

Leads that direct attack of a UOV system should be as hard as a random system were given in [6]. Intuitively, UOV$^{\hat{+}}$ is UOV with just extra random equations. So solving directly a UOV$^{\hat{+}}$ system is at least as hard as solving a UOV system with same parameters. The best way to solve directly a system such as $\mathcal{P}(x) = y$ is the hybrid approach, being understood that one must whatsoever start by

[6] This observation was brought to us by M. Øygarden and P. Briaud.

fixing v variables, hence getting a system of h equations in h variables. We recall here the complexity for solving a system of n equations in n variables, when fixing k additional variables:

$$\min_k \left(3q^k \binom{n-k+d_{\text{reg}}}{d_{\text{reg}}}^2 \binom{n-k}{2} \right)$$

where d_{reg} is the smallest integer d for which the coefficient of z^d in

$$\frac{(1-z^2)^n}{(1-z)^{n-k}}$$

is non-positive.

128 bit security								
q	3	4	5	8	16	59	277	983
n	83	71	65	57	50	45	42	41
192 bit security								
q	7	8	11	16	29	79	787	2179
n	92	90	85	80	75	70	65	64
256 bit security								
q	43	59	107	233	269	547	911	1433
n	100	98	95	92	91	90	89	88

Table 1: Sample values of (n, q) for which solving a random system of n quadratic equations in n variables in $\mathbb{F}_q$ with hybrid method exceed given complexity.

See Table 1 for sample parameters.

5.2 Direct UOV$^{\hat{+}}$ key recovery

A direct translation of the key recovery of a UOV$^{\hat{+}}$ is to find the "Oil" subspace, a subspace such that the restriction of the public equations to it, is a t dimensional space of quadratic equations. Notice that when $t = 0$, we retrieve the definition of the classic UOV problem: the public equations vanish on the Oil subspace. More formally, the problem is to find a basis of h vectors $(u_1, \ldots, u_h)$, such that the matrix with coefficients $\Delta\,\mathcal{P}_i(u_j, u_k)$ indexed by i for the rows, and (j, k) for the columns, has at most rank t. This problem can be directly put into equations: the basis of the Oil subspace can be supposed in row echelon form, so it can be expressed by the means of $h \times v$ unknown variables. Then the coefficients $\Delta\,\mathcal{P}_i(u_j, u_k)$ can be expressed as quadratic expressions of these variables (and linear in the coefficients of $\mathcal{P}$), and finally we can express that all the $(t+1)$-minors of the matrix vanish. Therefore, a rough estimation shows that we can get at most $\binom{h}{t+1}.\binom{\binom{h+1}{2}}{t+1}$ independent equations with $\binom{v^2\binom{h+1}{2}+t+1}{t+1}$ monomials.

A simple evaluation for various values shows that the number of monomials is always far beyond the number of equations, so simple linearization is completely out of reach.

To our best knowledge, we are not aware of other modellings that could lead to an efficient solving.

5.3 UOV attacks

We study here the possibility of performing a UOV-like rank attack on $\mathrm{UOV}^{\hat{+}}$, just as if we could pretend that the $\mathrm{UOV}^{\hat{+}}$ is merely a UOV system. Indeed, when selecting at random a linear combination of public equations, there is one chance out of q^t that the contribution of the $\hat{+}$ vanish. So the general idea is to pick up, let say, e equations that have one chance out of q^{et} to all belong to the pure UOV, perform an attack, then check if the result is consistent with the remaining equations. So, by performing in average q^{et} times the attack, we should find the key. In order to minimize q^{et}, we have to estimate e the minimum number of equations required to perform any kind of rank attack. Obviously, $e = 1$ is insufficient since one equation issued from a UOV system is indistinguishable from a random equation. More surprisingly, $e = 2$ is also not sufficient: any pair of random quadratic equation can always be interpreted as part of an OV system, see for instance [11], so in this case the attack would retrieve two many solutions. So, in a conservative setting, we estimate that an attacker need at least to pick up at least $e = 3$ many equations before attempting any UOV-like attack.

In a defensive point of view, it suffices then to select q and t such that $q^{3t} > 2^\lambda$ to be out of reach of any UOV-like attacks.

6 More efficient $\mathrm{UOV}^{\hat{+}}$: field extension & Petzoldt's public key compression

Using the idea presented in [8], it seems interesting to express the public key in a field extension (typically $\mathbb{F}_{q^t}$), so that the public key is t time smaller. Furthermore, the previous choice $q^{3t} > 2^\lambda$ helps also also to keep this feature safe. So in our settings, h and v are multiple of t, an irreducible polynomial f of degree t of $\mathbb{F}_q$ is chosen, and computations of the public equations can be performed over $\mathbb{F}_q[x]/(f)$. It is also possible to use the technique of public key compression given by Petzoldt et al. in [14], then the public key size amounts only to $(h-t)h(h+1)/2t \log_2 q$ bits. Our scheme is therefore quite competitive compared for instance to [3].

7 Signature mode, choice of parameters

7.1 $\mathrm{HFE}^{\hat{+}-}$

Security : 128 bits.
$q = 2, n = 263, r = 7 (d = 65), t = 6, a = 7.$

Signature size : 263 bits.
Public key size : 1111 Kbytes.
Signature time: 10s.

7.2 UOV$^{\hat{+}}$

Security : 128 bits.
$q = 2^6, h = 48, v = 56, t = 8$.
Hash size : 36 bytes.
Signature size : 78 bytes.
Public key size : 5 Kbytes.
Signature time: 0.7s.

Security : 192 bits.
$q = 2^9, h = 64, v = 72, t = 8$.
Hash size : 72 bytes.
Signature size : 153 bytes.
Public key size : 18 Kbytes.
Signature time: 1.5s.

Security : 256 bits.
$q = 2^{12}, h = 88, v = 96, t = 8$.
Hash size : 132 bytes.
Signature size : 276 bytes.
Public key size : 63 Kbytes.
Signature time: less than 4.0s.

References

1. John Baena, Pierre Briaud, Daniel Cabarcas, Ray Perlner, Daniel Smith-Tone, and Javier Verbel. Improving support-minors rank attacks: applications to gemss and rainbow. Cryptology ePrint Archive, Report 2021/1677, 2021. `https://ia.cr/2021/1677`.
2. Luk Bettale, Jean-Charles Faugere, and Ludovic Perret. Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic. *Designs, Codes and Cryptography*, 69(1):1–52, 2013.
3. Ward Beullens. Mayo: Practical post-quantum signatures from oil-and-vinegar maps. Cryptology ePrint Archive, Report 2021/1144, 2021. `https://ia.cr/2021/1144`.
4. Wieb Bosma, John Cannon, and Catherine Playoust. The Magma Algebra System I: The User Language. *Journal of Symbolic Computation*, 24(3):235–265, 1997.
5. Charles Bouillaguet, Pierre-Alain Fouque, Antoine Joux, and Joana Treger. A family of weak keys in HFE and the corresponding practical key-recovery. *Journal of Mathematical Cryptology*, 5(3-4):247–275, 2012.

6. Stanislav Bulygin, Albrecht Petzoldt, and Johannes Buchmann. Towards provable security of the unbalanced oil and vinegar signature scheme under direct attacks. *IACR Cryptol. ePrint Arch.*, page 420, 2010.
7. Jintai Ding and Bo-Yin Yang. Degree of regularity for HFEv and HFE$v-$. In *International Workshop on Post-Quantum Cryptography*, pages 52–66. Springer, 2013.
8. Hiroki Furue, Yasuhiko Ikematsu, Yutaro Kiyomura, and Tsuyoshi Takagi. A new variant of unbalanced oil and vinegar using quotient ring: QR-UOV. *IACR Cryptol. ePrint Arch.*, 2020:1243, 2020.
9. Aviad Kipnis, Jacques Patarin, and Louis Goubin. Unbalanced Oil and Vinegar signature schemes. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 206–222. Springer, 1999.
10. Mingjie Liu, Lidong Han, and Xiaoyun Wang. On the equivalent keys in multivariate cryptosystems. *Tsinghua Science and Technology*, 16(3):225–232, 2011.
11. Gilles Macario-Rat, Jérôme Plût, and Henri Gilbert. New insight into the isomorphism of polynomial problem IP1S and its use in cryptography. In Kazue Sako and Palash Sarkar, editors, *Advances in Cryptology - ASIACRYPT 2013 - 19th International Conference on the Theory and Application of Cryptology and Information Security, Bengaluru, India, December 1-5, 2013, Proceedings, Part I*, volume 8269 of *Lecture Notes in Computer Science*, pages 117–133. Springer, 2013.
12. Jacques Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 33–48. Springer, 1996.
13. Jacques Patarin, Louis Goubin, and Nicolas T. Courtois. C^{*-+} and HM: Variations around two schemes of T. Matsumoto and H. Imai. In *ASIACRYPT*, 1998.
14. Albrecht Petzoldt, Stanislav Bulygin, and Johannes Buchmann. Cyclicrainbow - A multivariate signature scheme with a partially cyclic public key. In Guang Gong and Kishan Chand Gupta, editors, *Progress in Cryptology - INDOCRYPT 2010 - 11th International Conference on Cryptology in India, Hyderabad, India, December 12-15, 2010. Proceedings*, volume 6498 of *Lecture Notes in Computer Science*, pages 33–48. Springer, 2010.
15. Chengdong Tao, Albrecht Petzoldt, and Jintai Ding. Improved key recovery of the HFE$v-$ signature scheme. *IACR Cryptol. ePrint Arch*, 1424, 2020.
16. Chengdong Tao, Albrecht Petzoldt, and Jintai Ding. Efficient key recovery for all HFE signature variants. In *Annual International Cryptology Conference*, pages 70–93. Springer, 2021.