Onyx: New Encryption and Signature Schemes with Multivariate Public Key in Degree 3

Gilles Macario-Rat[1] and Jacques Patarin[2]

[1] Orange, Orange Gardens, 46 avenue de la République, F-92320 Châtillon, France
gilles.macariorat@orange.com
[2] Versailles Laboratory of Mathematics, UVSQ, CNRS, University of Paris-Saclay
jpatarin@club-internet.fr

Abstract. In this paper, we present a new secret trapdoor function for the design of multivariate schemes that we call "Onyx", suitable for encryption and signature. It has been inspired by the schemes presented in [19,20]. From this idea, we present some efficient encryption and signature multivariate schemes with explicit parameters that resist all known attacks. In particular they resist the two main (and often very powerful) attacks in this area: the Gröbner attacks (to compute a solution of the system derived from the public key) and the MinRank attacks (to recover the secret key). Specific attacks due to the properties of the function and its differential are also addressed in this paper. The "Onyx" schemes have public key equations of degree 3. Despite this, the size of the public key may still be reasonable since we can use larger fields and smaller extension degrees. Onyx signatures can be as short as the "birthday paradox" allows, i.e. twice the security level, or even shorter thanks to the Feistel-Patarin construction, like many other signatures schemes based on multivariate equations.

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

1 Introduction

Many schemes in Multivariate cryptography have been broken. Among the most spectacular attacks we can mention that the C scheme of Matsumoto and Imai [21] has been broken in [22], the SFlash scheme submitted to the NESSIE competition has been broken in [7,13,14] , the LUOV scheme [4] submitted to the Post-Quantum NIST competition has been broken in [11], and the GeMMS schemes [8] has been broken in [26]. At present the two main general attacks in multivariate cryptography are the use of Gröbner bases in "direct attacks" (in order to find a solution of the public equations involved without finding the secret key, cf [15]), and the MinRank attacks in order to find the secret key [17,3]. In many schemes the Gröbner attack is dangerous because the degree of regularity of the public equations is smaller than for random quadratic equations. Recently the MinRank attacks have become much more powerful than before due to the introduction of the Minor equations [3].

Despite these dangerous and powerful attacks, multivariate cryptography remains an interesting area of research. This is mainly due to three facts. First, the schemes, if they can resist non-quantum attacks, are also expected to resist quantum computers, i.e. multivariate cryptography is one of the family of "post-quantum" cryptography (with lattices, codes, hash-based cryptography, isogenies, combinatorial schemes). Second, the MQ problem (solving a set of Multivariate Quadratic equations on finite field) is NP-hard on any finite field, and seems to be very difficult to solve when the equations are random and the number of variables is about the same as the number of equations. Third, some properties can be obtained at present only with multivariate cryptography such as ultra-short public-key signatures, or encryption with ultra-short blocs [24].

It is also interesting to notice that multivariate schemes (like many secret key schemes) can benefit from small changes in their design (tweaks, perturbations, etc.), offering them the ability to thwart otherwise dangerous attacks. See for example Gemss [8].

Note also that it is in general much easier to design a signature scheme than an encryption scheme: indeed at present, very few encryption candidates are available. Hopefully, Onyx will be able to perform both modes.

2 Onyx: main ideas

2.1 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 $(x_1, \dots, x_n)$ (or simply $\bar{x}$) over $\mathbb{F}_q$, noted $\mathbb{F}_q[\bar{x}]$ (implicitly modulo $(x_1^q - x_1, \dots, x_n^q - x_n)$). Therefore here $\mathbb{F}_q[\bar{x}]^m$ will refer to the algebra of n-ary m-dimensional polynomials, that we call (n, m)-polynomials for short. The internal product of this algebra is implicitly defined as the extension of the product defined over $\mathbb{F}_q^m$, itself defined by the classical (field) product over $\mathbb{F}_{q^m}$ and transferred by a proper isomorphism $\varPhi : \mathbb{F}_{q^m} \to \mathbb{F}_q^m$. By extension, for $\alpha \in \mathbb{F}_{q^m}$, we denote $\bar{\alpha} = \varPhi(\alpha)$, $\bar{\alpha} \in \mathbb{F}_q^m$. We denote φ the Frobenius mapping $\varphi : \mathbb{F}_{q^m} \mapsto \mathbb{F}_{q^m},\ x \to x^q$; the multipliers mappings $\varLambda_\alpha$, $\alpha \in \mathbb{F}_{q^m}$: $\varLambda_\alpha : \mathbb{F}_{q^m} \mapsto \mathbb{F}_{q^m},\ x \to \alpha x$; and finally the well known linear mapping "trace", $\mathrm{Tr} : \mathbb{F}_{q^m} \mapsto \mathbb{F}_q,\ x \to \sum_{i=0}^{m-1} x^{q^i}$.

When $n = m$, for a function $F : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$, we denote $\tilde{F} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ where $\tilde{F} = \varPhi \circ F \circ \varPhi^{-1}$. For instance, the frobenius φ is a linear polynomial of degree q of $\mathbb{F}_{q^n}[x]$, whereas $\tilde{\varphi}$ is a linear (n, n)-polynomial of degree 1 of $\mathbb{F}_q[\bar{x}]^n$.

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

We use $\mathcal{M}_n(\mathbb{F}_q)$ to denote the set of square $n \times n$-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 $\bar{x}$ is a (row) vector, then $\bar{x}^{\mathrm{t}}$ 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/` [5]. Time measurement were performed on an Intel Core i7-6700 CPU, 3.4GHz, with a C++ program developed under Microsoft Visual Studio 2019.

2.2 The Onyx trapdoor and first properties

The Onyx function, following the example of HFE, specifically exploits the construction of small field and big field. Here we will use odd characteristics > 3, q will be therefore a small odd prime or odd prime power, typically $q = 59$. The extension degree should also be preferably odd, such as $n = 47$, and $m = n$. In what follows, whenever it makes sense, we have implicitly $\bar{x} = \Phi(x)$.

We define our Onyx function F as a univariate polynomial over $\mathbb{F}_{q^n}$:

$$F(x) = \alpha x^3 + \beta p(\bar{x})x, \tag{1}$$

where α, β are random elements of $\mathbb{F}_{q^n}$ and p is a homogeneous degree-2 $(n, 1)$-polynomial of $\mathbb{F}_q[\bar{x}]$. That is to say we can express $p(\bar{x}) = \sum_{i,j} a_{ij} x_i x_j$, where $\{a_{ij}\}$ are random elements of $\mathbb{F}_q$. It is worthwhile to note that we could also express $p(\bar{x}) = \mathrm{Tr}(\sum_{i,j} \alpha_{ij} x^{q^{i+j}})$, with some other elements $\{\alpha_{ij}\}$ of $\mathbb{F}_{q^n}$ (depending of $\{a_{ij}\}$). This latter expression shows that the degree of $p \circ \Phi$ and hence also F, is not bounded by a small value, but can be as big as $2q^{n-1}$, contrary to the trapdoor functions of HFE.

We can note also that, due to the particular expression of F, $\tilde{F}$ is a degree-3 homogeneous (n, n)-polynomial. Classically, we can use two additional bijective linear secret mappings S and T of $\mathbb{F}_q^n$, and publish $\mathcal{P} = S \circ \tilde{F} \circ T$, which also will be a degree-3 homogeneous (n, n)-polynomial.

2.3 Equivalent keys

The study of equivalent keys is important to assess the security of a multivariate scheme (see [18]). 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”. Notice that whatever the linear mapping τ, then $p' = p \circ \tilde{\tau}$ is eligible for the Onyx scheme. It follows that if $\sigma \circ F \circ \tau$ is eligible for the scheme, then $(S \circ \tilde{\sigma}^{-1}, \tilde{\tau}^{-1} \circ T, \sigma \circ F \circ \tau)$ is obviously an equivalent key. Among the sustainders, are the multipliers: Λ_γ, $\gamma \in \mathbb{F}_{q^n}$ and the iterates of the Frobenius: $\varphi^{(i)} : x \to x^{q^i}$. Since we have: $\Lambda_\gamma \circ (\alpha x^3 + p(\bar{x})\beta x) \circ \Lambda_\delta = \alpha\gamma\delta^3 x^3 + p(\Phi(\delta x))\beta\gamma\delta x$, by choosing $\delta = \sqrt{\beta/\alpha}$,

$\gamma = 1/\beta\delta$, we see that there exists always an equivalent key with $\alpha' = \beta' = 1$([3]). So from now, we may consider that the secret Onyx function is simply

$$F(x) = x^3 + p(\bar{x})x, \tag{2}$$

where p is still a homogeneous degree-2 polynomial of $\mathbb{F}_q[\bar{x}]$, moreover unitary (the coefficient of its leading monomial, for a given monomial order, is 1). With this new definition, the equivalent keys are most probably only the $n-1$ ones induced by the iterated Frobenius $(\sigma, \tau) = (\varphi^{(i)}, \varphi^{(n-i)})$, $i = 1, \ldots, n-1$, and the $q-1$ ones induced by the "small" multipliers $(\sigma, \tau) = (\Lambda_{1/a^3}, \Lambda_a)$, $a \in \mathbb{F}_q,\ a \neq 0$.

2.4 Weak keys

Following the example of [6], 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 : $A = T^{-1} \circ \tilde{\tau}^{-1} \circ T$, and $B = S \circ \tilde{\sigma} \circ S^{-1}$. 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 p satisfying for all $x \in \mathbb{F}_q^n,\ p \circ \tilde{\varphi}(\bar{x}) = p(\bar{x})$ (this is the case for instance if $p(\bar{x}) = \mathrm{Tr}(x^{q^i+q^j})$) leads indeed to a weak key. Since p may be chosen at random, it is very unlikely that it fulfills this condition.

2.5 Rank of the Onyx function

An important aspect of the Onyx function is its rank, since any rank defect in the public key due to the secret function could be exploited by an attacker. Here since the public equations are degree-3 polynomials, we must explain what kind of rank we are talking about. 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 $P(x) = \sum_{i=1}^{r} L_{i1}(x)L_{i2}(x)$. By extension, the rank of a degree-3 polynomial P is the minimum number r of products of three linear polynomials L_{ij}, $j = 1, 2, 3$, in the possible sums $P(x) = \sum_{i=1}^{r} L_{i1}(x)L_{i2}(x)L_{i3}(x)$. Since we have $F(x) = x(x^2 + p(\bar{x}))$, and since p is randomly chosen, we may assume that with overwhelming probability, $x^2 + p(\bar{x})$ has rank n and therefore, F has also rank n.

Notice also that, although the computation of the rank of a degree-2 polynomial (i.e. quadratic) is well known and has polynomial complexity, the computation of the rank of a degree-3 (cubic) polynomial is a NP-Hard problem.[4]

[3] If β/α is not a square, there must exist $l \in \mathbb{F}_q,\ l \neq 0$ such that $l\beta/\alpha$ is a square. Therefore consider $\alpha' = \alpha, p' = p/l, \beta' = l\beta$, which leads of course to the same F.

[4] Degrees 2 and 3 behave totally differently: for instance, the maximum rank of a cubic form is unknown, the best known upper bound is $\lceil (3/4)n^2 \rceil$, see [2].

2.6 Special inversion of the Onyx function

The special shape of the Onyx function was chosen such that it is of course possible to efficiently inverse it, that is to efficiently and practically compute the solutions in x of the equation $F(x) = y$, for any given y in $\mathbb{F}_{q^n}$. Since the degree of F is huge (possibly $2q^{n-1}+1$), a direct method such as the Berlekamp algorithm cannot be used primarily. On the other hand, we can exploit the property of p which is in $\mathbb{F}_q[\bar{x}]$. Moreover, we have chosen q small enough, so that it is possible to make an exhaustive search of the value of $p(\bar{x})$ which can take only q possibilities. Therefore, a first method to solve $F(x) = y$ is to solve the q equations $x^3 + rx = y$, $r \in \mathbb{F}_q$, (easy to solve, since degree-3 polynomials), and keep the solutions satisfying $p(\bar{x}) = r$. A second method involves the elimination of $p(\bar{x})$ by using the natural field equation: for all x in $\mathbb{F}_{q^n}$, $p(\bar{x})^q = p(\bar{x})$. Hence we get

$$x^{3q} - x^{q+2} + yx^{q-1} - y^q = 0 \tag{3}$$

which can be solved using Berlekamp algorithm for a degree-$3q$ polynomial. Theory and experiments show that solving q degree-3 polynomials (first method) is a little bit more efficient than solving one degree-$3q$ polynomial (second method).[5]

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. The only difference with a random equation is that it cannot have more than $3q$ solutions (due to its special form) but the probability to observe a random equation with so many solutions is very low.

3 Security analysis

3.1 Direct attacks

At the light of [10], we think that by choosing odd q big enough, we are safe from the algebraic attacks that aims to invert directly the system using Gröbner basis computation. Indeed, experiments with small values of n show that the degree of regularity of the system $\tilde{F}(\bar{x}) = \bar{y}$ (without field equation) is $2n + 1$, which is also the degree of regularity of a random system of degree 3 with same dimensions (number of variables and equations). If we include the field equations $x_i^q = x_i$, we again observe the same degree of regularity with our system and a random system of same dimensions with field equations added. We therefore estimate that the hybrid attack (mix of exhaustive search and Gröbner basis computation) is the best option for an attacker. See Table 1 for the complexity of the Hybrid attack. Note that in the case of the signature mode, we choose to have $q^n \approx 2^{2\lambda}$, which raises values of n much higher than what is needed to be above the attack (at least for values of q less than 800). For encryption mode, minimum values of n that are equal to or just above the threshold of the attack can be chosen.

[5] We can even use the Cardano's formula since we deal with cubics (see Sec. A).

q	n	C	D_{reg}	k	q	n	C	D_{reg}	k	q	n	C	D_{reg}	k
11	41	132.09	9	23	11	65	204.24	13	35	11	83	257.85	17	42
23	35	131.00	13	13	23	53	194.88	15	23	23	71	256.87	20	29
59	31	130.33	16	8	59	47	192.92	26	9	59	65	262.00	29	16
131	29	128.88	19	5	131	47	203.28	26	9	131	61	260.70	35	10

Table 1. Complexity ($\log_2$) of hybrid attack for various random systems of n degree-3 equations in n variables in $\mathbb{F}_q$, k: number of variables to fix for the best trade-off, D_{reg}: degree of regularity for the best trade-off, $C = q^k \binom{n-k+D_{reg}}{D_{reg}}^{\omega}$, $\omega = 2.37$

3.2 Rank attacks

Onyx was designed as the combination of a HFE-like polynomial, i.e. with bounded degree, and a dense non-bounded degree polynomial which may in some sense "vanish" at inversion time. As a desired effect, the secret function has rank n. We know that by eliminating p, we can get

$$F(x)^q x - F(x) x^q = x^{3q+1} - x^{q+3}. \tag{4}$$

Said otherwise, there exists an equation satisfied by the secret function, and hence also by the public equation, with small rank (it is the sum of only 2 products involving only x and x^q). However, it is not possible to exploit it by mounting an efficient MinRank attack. Indeed, if we transpose (4) into the public space, we get the following "modified" MinRank Problem: find coefficients of S^{-1} and T defined by $\sum t_i x^{q^i} = T(x)$ and $\sum s_i x^{q^i} = S^{-1}(x)$, such that $\sum_{i,j} (s_{i-1}^q t_j - s_i t_{j-1}^q)\, \mathcal{P}^{q^i}\, x^{q^j}$ has low rank. We believe that this problem has an exponential complexity, since it is clearly quadratic in the unknowns (s_i) and (t_i).

3.3 Key recovery attacks, differential and specific attacks

The differential is a very useful tool that gives a strong insight of a function. It has been very useful for various cryptanalysis (see for instance [16,25,12].) The differential of a function f at a point k is defined as: $\Delta_k\, f(x) = f(x+k) - f(x) - f(k) + f(0)$. When f is quadratic, it is well known that $\Delta_k\, f$ is linear function. When f is cubic, there exists a function $\Delta^{(2,1)}\, f(k,x)$, quadratic in k and linear in x such that: $\Delta_k\, f(x) = \Delta^{(2,1)}\, f(k,x) + \Delta^{(2,1)}\, f(x,k)$. In the particular case of the Onyx function, we have $F(x) = x^3 + p(\bar{x})x$. First we can write $p(\bar{x}) = \bar{x}.M.\bar{x}^{\mathrm{t}}$, where M is some symmetric matrix of $\mathcal{M}_n(\mathbb{F}_q)$. Then we get :

$$\Delta^{(2,1)}\, F(k,x) = 3k^2 x + p(\bar{k})x + 2(\bar{k}.M.\bar{x}^{\mathrm{t}})k. \tag{5}$$

The properties of the differential of the secret Onyx function are transferred to the public equations due to the relation $\mathcal{P} = S \circ \tilde{F} \circ T$. Then, we get : $\Delta^{(2,1)}\, \mathcal{P}(k,x) = S(\Delta^{(2,1)}\, \tilde{F}(T(\bar{k}), T(\bar{x})))$ or equivalently: $\Delta^{(2,1)}\, \mathcal{P}(\bar{k},.) = S \circ$

$\Delta^{(2,1)}\,\tilde{F}(T(\bar{k}),.)\circ T$, which means that $\Delta^{(2,1)}\,\mathcal{P}(k,.)$ and $\Delta^{(2,1)}\,\tilde{F}(T(\bar{k}),.)$ are linearly equivalent. A thorough analysis shows that the linear mapping $\Delta^{(2,1)}\,F(k,.)$ is most of the time regular (full rank), and some times has rank $n-1$. (From now on, we implicitly do not consider the trivial case $k=0$.) In the latter cases indeed, its kernel is a vector line with basis $k_0 = k/(3k^2+p(\bar{k}))$, and the condition $2(\bar{k}.M.\bar{k}_0^{\mathrm{t}}) = -1$ is met, which has roughly the probability $1/q$ to occur. To be complete, we must say that the number of k that cancel $3k^2+p(\bar{k})$ is negligible (at most the q elements of $\mathbb{F}_q$), and may be even zero if $p(1)\neq -3$.

This knowledge in mind, by picking at random values k and computing whenever possible a vector k_0 in the kernel of $\Delta^{(2,1)}\,\mathcal{P}(k,.)$, we then get some relations involving known values k and k_0 and the secret parameters T and p:

$$3T(\bar{k}_0)T(\bar{k})^2 + p(T(\bar{k}))T(\bar{k}_0) + 2(T(\bar{k}).M.T(\bar{k}_0)^{\mathrm{t}})T(\bar{k}) = 0. \tag{6}$$

We can get a lot of such equations by picking all possible values k, however the dimension of the space spanned by them is of course limited. Since the n coefficients of k appear in the equations with degree 1 and the n coefficients of k_0 appear with degree 2, the dimension is bounded by $n\binom{n}{1}\binom{n+1}{2}$, which is $O(n^4)$. The equations can be expressed in the n^2 coefficients of T in degree 3 and the $n(n+1)/2$ coefficients of p (or M) in degree 1, which raises $O(n^8)$ monomials of degree 4 in the unknowns. We estimate that these systems have a (huge) exponential complexity (see Sec. B).

An other idea may be to get rid of p and M in these equations by using the field equation. We get then :

$$\begin{aligned} &T(k_0)^{q^2+q}T(k)^{2q+1} + T(k_0)^{q^2+1}T(k)^{2q^2+q} + T(k_0)^{q+1}T(k)^{q^2+2} \\ &\quad - T(k_0)^{q^2+q}T(k)^{2q^2+1} - T(k_0)^{q+1}T(k)^{q^2+2q} - T(k_0)^{q^2+1}T(k)^{q+2} = 0. \end{aligned} \tag{7}$$

These equations can be expressed in the n^2 unknown coefficients of T and the $2n$ coefficients of k and k_0. They are homogeneous of degree 10: degree 5 in T, 3 in k and 2 in k_0. So we get $O(n^{10})$ unknown monomials and the number of independent equations is bounded by $n\binom{n+1}{2}\binom{n+2}{3} = O(n^6)$. Again we estimate (see Sec. B) that solving these systems is less complex than the previous ones, but nevertheless, has still an exponential complexity.

We can take an other path, knowing that among all the equations (6), about one out of q may satisfy $p(T(\bar{k}))=0$ (although we have no way to know which ones). Then we would get a set of equations of the kind

$$3T(\bar{k}_0)T(\bar{k}) + 2(T(\bar{k}).M.T(\bar{k}_0)^{\mathrm{t}}) = 0. \tag{8}$$

Suppose that we collect N couples (k,k_0) satisfying equation (6) and select a fraction $1/q$ of them supposedly satisfying (8), and suppose we could retrieve T, even at no cost, the attack would cost at least a factor $\binom{N}{N/q}$, which is exponential since we should have $N/q > n^2$ (at least more equations than the unknown number of coefficients of T).

All in all, it seems that this very specific property of the kernel of the differential does not raise a system that can be solved efficiently nor can retrieve information of the secret key.

4 Signature mode

The Onyx function is appropriate for a signature scheme, with a small drawback due to the fact that the Onyx function may not have a pre-image, the failure rate is then the fraction of such cases.

As it is, we have seen that the probability that a random polynomial function has no pre-image on a random value is about $1/e$ or $0,37\%$. We verified experimentally that the Onyx function follows approximately this rule.

To circumvent the failure rate, a first option is the following: let h be the hash of the message M to be signed, draw a random string r, until $F(x) = S^{-1}(h\|r)$ has a solution. Then the signature is $T^{-1}(x)\|r$. To verify a signature $\sigma\|r$ of a message M, compute h the hash of M, and then just check that $\mathcal{P}(\sigma) = h\|r$. The length of the random string r should be chosen such that the resulting failure rate become negligible ($\approx \lceil \log_2 \lambda \rceil$ bits)[6].

A second option is to introduce "vinegar" variables in the secret scheme. The Onyx function with vinegar becomes:

$$F(x, \bar{x}') = x^3 + (p(\bar{x}\|\bar{x}') + \varPhi^{-1}(Q(\bar{x}'))x + \varPhi^{-1}(C(\bar{x}')), \tag{9}$$

where $\bar{x}'$ is a vector of v variables of vinegar, Q and C are respectively degree-2 and degree-3 (v, n)-polynomials, p is now a degree-2 $(n + v, 1)$-polynomial. We must also adapt T which is now a $\mathbb{F}_q^{n+v}$ linear mapping. The general idea is obviously that when $\bar{x}'$ is set, the equation in $F(x, x') = y$ can be solved efficiently in x. Again, choose the number of vinegar variables big enough, so the failure rate become negligible (for instance chose v such that $q^v > \lambda$)[6]. To sign a message with hash h, compute $\bar{y} = S^{-1}(h)$, draw at random $\bar{x}'$ until $F(x, x') = \bar{y}$ has a solution in x, and finally a signature is $\sigma = T^{-1}(\bar{x}\|\bar{x}')$. To verify a signature σ of a message M, compute h the hash of M, and then just check that $\mathcal{P}(\sigma) = h$.

See Table 2 for possible parameters for signature mode.

In tables 2,3,4, we present the times in two columns, one is named "Serial" : we assume that all calculations are carried out consecutively. The second one is named "Parallel" : we assume that calculations are carried out in different threads simultaneously. So roughly, for verification and encryption the parallel time is the time required to evaluate one single public equation, (so it is evaluated as the serial time divided by n); for decryption and signature the parallel time is the time required to compute the roots of one single polynomial (so it is evaluated as the serial time divided by q). These times could be of course greatly improved according the platform, or by hardware since computations only require common operations in the field $\mathbb{F}_q$.

[6] The failure rate after λ attempts is $e^{-\lambda} \ll 2^{-\lambda}$.

λ	q	n	Verification		Signature		Pub. Key	Sig. size
Security Bits			Serial	Parallel	Serial	Parallel	KBytes	Bits
128	11	77	7.5ms.	0.1s.	2.2ms.	0.2ms.	3045	267
128	23	59	2.5ms	43μs.	3.4ms.	0.15ms.	1328	267
128	59	47	1.0ms.	22μs.	5.6ms.	0.1ms.	650	277
128	131	37	0.3ms.	9μs.	8ms.	60μs.	339	261
192	59	67	4.3ms.	64μs.	11.5ms.	0.2ms.	2633	395
192	131	55	2.0ms.	35μs.	16ms.	0.12ms.	1610	387
256	59	89	13.0ms.	0.15ms.	19ms.	0.35ms.	8110	524
256	131	73	6.0ms.	80μs.	28ms.	0.22ms.	4930	514

Table 2: Various parameters for signature mode. Signature involves here the Cardano's formulas and does not include the length of a random string which is whatsoever small (≈ 8 bits).

5 Encryption mode

The Onyx function is also suitable for encryption mode. However, a slight drawback is that the decryption may return more than one value. There are fortunately several ways to deal with that, by using an authentication function H for instance. First option (external MAC): to encrypt a message x, one sends $(\bar{y}, h) = (\mathcal{P}(\bar{x}), H(x))$. To decrypt a message $(\bar{y}, h)$, for each solution of $F(x) = \Phi^{-1}(S^{-1}(\bar{y}))$, compute $\bar{z} = T^{-1}(\bar{x})$ and return the value z that matches $H(z) = h$. Second option (internal MAC): to encrypt a message x, send $\bar{y} = \mathcal{P}(\bar{x} \| H(x))$. To decrypt a message $\bar{y}$, for each solution of $F(x) = \Phi^{-1}(S^{-1}(\bar{y}))$, compute $(\bar{z} \| h) = T^{-1}(\bar{x})$ and return the value z that matches $H(z) = h$.

See Table 3 for possible parameters for encryption mode.

λ	q	n	Encryption		Decryption		Pub. Key	Block. size
Security Bits			Serial	Parallel	Serial	Parallel	KBytes	Bits
128	11	41	0.5ms.	12μs.	0.6ms.	60μs.	253	141
128	23	35	0.3ms.	9μs.	1.2ms.	50μs.	170	158
128	59	31	0.2ms.	6μs.	2.8ms.	50μs.	127	182
128	131	29	0.15ms.	5μs.	6.0ms.	50μs.	131	203
192	59	47	1.0ms.	30μs.	6.0ms.	0.1ms.	650	276
256	59	65	4.0ms.	65μs.	9.5ms.	0.16ms.	2336	382
256	131	61	3.0ms.	50μs.	22ms.	0.17ms.	2423	429

Table 3: Various parameters for encryption mode. Decryption involves here the Cardano's formulas.

6 Short signatures

In the case of Onyx, it seems profitable to take advantage of the parameters of the encryption mode and use them in signature mode, by the mean of the iteration process used for instance in Gemss ([8]) or Quartz ([23]) also called the "Feistel-Patarin" mode. The idea is to avoid the birthday paradox attack, while keeping a signature size below the double of the security level, by chaining many inversion processes of the secret function. For L rounds, L values $Y_1, \ldots, Y_L$ are derived from the hash of the message to sign, and then $L+1$ values $X_0, \ldots, X_L$ are computed, satisfying $X_0 = 0$, and $\mathcal{P}(X_i) = Y_i \bigoplus X_{i-1}$, for $i = 1, \ldots, i = L$, and finally X_L is the signature. To produce a signature indeed, the inversion of the secret function is used L times. To verify a signature, the L values $Y_1, \ldots, Y_L$ are computed from the message, the $L+1$ values $X_0, \ldots, X_L$ are computed in reversed order, starting with X_L equal to the signature and then $X_{i-i} = \mathcal{P}(X_i) \bigoplus Y_i$, for $i = L, \ldots, 1$. The signature is valid if and only if X_0 is 0. For a security level λ, and a block size b (input) of the secret function, the number L of iterations must be chosen such that (see [23] or [8]) :

$$b\frac{L}{L+1} \geq \lambda.$$

λ Bits	q	n	L Rounds	Verification		Signature		Pub. Key KBytes	Sig. size Bits
				Serial	Parallel	Serial	Parallel		
128	11	41	10	5ms.	0.15ms.	6.5ms.	0.6ms.	253	171
128	23	35	5	1.5ms.	40μs.	6.0ms.	0.25ms.	170	183
128	59	31	3	0.5ms.	20μs.	9.0ms.	0.15ms.	127	200
128	131	29	2	0.3ms.	10μs.	11.0ms.	80μs.	131	217
192	59	47	3	3.0ms.	60μs.	16.0ms.	0.3ms.	650	294
256	59	65	3	12.0ms.	0.2ms.	30.0ms	0.5ms.	2336	400
256	131	61	2	5.5ms.	0.1ms.	42.0ms	0.3ms	2423	443

Table 4: Various parameters for short signature.

In table 4, times are deduced from those of table 3 by the following formulas : Verification time is Encryption time $*$ L. Signature time is Decryption time $*$ $L/(1 - e^{-1})$ (to take the failure rate into account). Signature size is : Block size + $L\lceil\log_2(\lambda)\rceil$ (to take into account a random string for dealing with failures). Notice that ($q = 59, n = 31$) and ($q = 131, n = 29$) give very efficient schemes compared to Gemss for instance.

A Cardano's formula for depressed cubic

Let $x^3 + ax + b = 0$ a so-called "depressed" cubic to solve in an algebraic closed field with characteristic $\neq 2, 3$. Let δ be a square root of $b^2 + 4a^3/27$ and u, v

be cubic roots of $(-b+\delta)/2$ and $(-b-\delta)/2$ satisfying $uv = -a/3$. Let j be a solution of $x^2+x+1=0$, then according to Cardano's formula, the three solutions of $x^3+ax+b=0$ are $u+v, uj+vj^2, uj^2+vj$.

More specifically, to get the solutions of the cubic in a particular field $\mathbb{F}_{q^n}$, we need to compute square and cubic roots in this field, and possibly in higher extensions. In order to have simple and deterministic computations, we make the following choices: $q^n \equiv 3 \mod 4$ and $q^n \equiv 2$ or $5 \mod 9$. Notice that with this choices, e_2, e_3 and e_3' defined hereafter, are integers. With these parameters also, computations require at most a quadratic extension. Indeed, in these fields -1 is not square (Euler's criterion), and 3 is a square (law of quadratic reciprocity). So we can define a quadratic extension $\mathbb{F}_{q^n}[i]$ where i satisfies $i^2=-1$. In this extension, we have $j = (\sqrt{3}i-1)/2$ and $j^2 = (-\sqrt{3}i-1)/2$ where $\sqrt{3}$ is a square root of 3 in $\mathbb{F}_q$. Moreover, let $e_2 = ((q^n-1)+2)/4$. For all y in $\mathbb{F}_{q^n}$ we have $0 = (y^{e_2})^4 - y^2 = ((y^{e_2})^2 - y)((y^{e_2})^2 + y)$, so the square roots of y are either $\pm y^{e_2}$ in $\mathbb{F}_{q^n}$ or $\pm i y^{e_2}$ in $\mathbb{F}_{q^n}[i]$. Finally, let $e_3 = (2(q^n-1)+1)/3$ and $e_3' = (2(q^{2n}-1)+3)/9$.[7] For all y in $\mathbb{F}_{q^n}$, $y = (y^{e_3})^3$, so y is a cube and y^{e_3} is its cubic root. For all y in $\mathbb{F}_{q^n}[i]$ we have $0 = (y^{e_3'})^9 - y^3 = ((y^{e_3'})^3 - y)((jy^{e_3'})^3 - y)((j^2y^{e_3'})^3 - y)$. Since j and j^2 are not cubes in $\mathbb{F}_{q^n}[i]$([8]) then if y is a cube in $\mathbb{F}_{q^n}[i]$, $y^{e_3'}$ and $jy^{e_3'}$ and $j^2y^{e_3'}$ are its three cubic roots in $\mathbb{F}_{q^n}[i]$.

For example, to compute the solutions of $x^3+ax+b=0$ in $\mathbb{F}_{59^{47}}$, we first compute a square root of 3 in $\mathbb{F}_{59}$: $\sqrt{3} = 48$, so $j = (48i-1)/2$. Then we compute $\Delta = b^2 + 4a^3/27$ and $\delta = \Delta^{e_2}$ in $\mathbb{F}_{59^{47}}$. If $\delta^2 = \Delta$, then the cubic has only one solution given by: $((-b+\delta)/2)^{e_3} + ((-b-\delta)/2)^{e_3}$. Otherwise we compute $U = (-b+i\delta)/2$ and $u = u_0 + iu_1 = U^{e_3'}$ (in $\mathbb{F}_{59^{47}}[i]$). If $u^3 = U$, then the cubic has three solutions in $\mathbb{F}_{59^{47}}$ given by $2u_0, -u_0+\sqrt{3}u_1, -u_0-\sqrt{3}u_1$. Otherwise the cubic has zero solution in $\mathbb{F}_{59^{47}}$.

A.1 Primitive ninth root of unity in $\mathbb{F}_q$

We suppose there exists an element j in a field $\mathbb{F}_q$ that satisfies $j^2+j+1=0$, q not being a power of 2 or 3, and would like to know on which condition upon q the cubic roots of j and j^2 are also in $\mathbb{F}_q$. There are six of these roots, which are also the roots of the polynomial $p_j(x) = x^6+x^3+1$. A simple proof by induction shows that for $l > 1$, $\gcd(x^l - x, p_j) = p_j$ if $l \equiv 1 \mod 9$ and 1 otherwise. Therefore, the answer is simple: the cubic roots of j are in $\mathbb{F}_q$ if and only if $q \equiv 1 \mod 9$.

B XL algorithm and its complexity

In section 3.3 we are lead to evaluate the complexity for solving systems with very large number of unknowns and equations. Since they are over-defined (more equations than unknowns), they have most probably few solutions but they have

[7] if $q^n \equiv 2 \mod 9$, or $e_3' = ((q^{2n}-1)+3)/9$ if $q^n \equiv 5 \mod 9$.

[8] $\mathbb{F}_{q^n}[i]$ has q^{2n} elements and $q^{2n} \equiv 4$ or $7 \mod 9$, see Sec. A.1

also large degrees, which makes difficult to evaluate their complexity. By fixing a few unknowns, we can assume that a system has always 0 or 1 solution. So, we suppose in this section that we want to solve a non-homogeneous system of m equations of degree d in n variables over $\mathbb{F}_q$ which has probably one solution. We follow here the idea of [9], which is to solve the system by linearization, that is, find the smallest degree D such that, when multiplying all equations by all monomials of degree $D - d$, we get more new equations than new monomials (of degree at most D). Then linearization amounts to compute the row echelon form of a matrix, hence the presence of ω in the formula of complexity.

Instead of finding a generic formula for D, it seems more appropriate to search it with a simple routine, by try and error, since most probably in our cases, D is bounded by n (or a polynomial function in n). Results corresponding to values (q, n) of Table 3 are summarized in Table 5.

It has been shown that XL may be not as efficient as F4/F5 (see [1]), however the results in Table 5 are so high that even if results with F4/F5 were half of those, they would not still be threatening.

q	n	λ	C_1	D_1	C_2	D_2
11	41	128	1189.38	78	575.06	35
23	35	128	983.68	67	488.06	31
59	31	128	853.63	60	426.82	28
131	29	128	795.01	57	402.51	27
59	47	192	1400.43	89	649.57	38
59	65	192	2046.13	121	905.45	49
131	61	256	1901.31	114	854.53	47

Table 5. Complexity C_i ($\log_2$) and degree D_i of the XL attack for systems ($i = 1$) issued from equations (6) and systems ($i = 2$) from equations (7), $\omega = 2.37$.

Addendum

We have afterwards realized that the differential (see Sec. 3.3 and (5)) of a degree-3 public key behaves somehow in the same manner as a degree-2 public key of another system. Therefore let's consider instead $F(x) = x^2 + p(\bar{x})\alpha$ where α is a random element of $\mathbb{F}_{q^n}$ and p is a homogeneous degree-2 $(n, 1)$-polynomial of $\mathbb{F}_q[\bar{x}]$. This will be the subject of an upcoming article about a degree-2 version of Onyx. We will explain that in fact the use of the "minus" modification (removing a few public equations) is required to thwart the minrank attack. Furthermore, since public keys are degree-2 type, then they are even significantly smaller.

References

1. Gwénolé Ars, Jean-Charles Faugere, Hideki Imai, Mitsuru Kawazoe, and Makoto Sugita. Comparison between XL and Gröbner basis algorithms. In *International*

Conference on the Theory and Application of Cryptology and Information Security, pages 338–353. Springer, 2004.

2. John Baena, Daniel Cabarcas, Daniel E. Escudero, Karan Khathuria, and Javier Verbel. Rank analysis of cubic multivariate cryptosystems. In *International Conference on Post-Quantum Cryptography*, pages 355–374. Springer, 2018.
3. Magali Bardet, Maxime Bros, Daniel Cabarcas, Philippe Gaborit, Ray A. Perlner, Daniel Smith-Tone, Jean-Pierre Tillich, and Javier A. Verbel. Improvements of algebraic attacks for solving the rank decoding and minrank problems. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part I*, volume 12491 of *Lecture Notes in Computer Science*, pages 507–536. Springer, 2020.
4. Ward Beullens and Bart Preneel. Field lifting for smaller UOV public keys. In Arpita Patra and Nigel P. Smart, editors, *Progress in Cryptology - INDOCRYPT 2017 - 18th International Conference on Cryptology in India, Chennai, India, December 10-13, 2017, Proceedings*, volume 10698 of *Lecture Notes in Computer Science*, pages 227–246. Springer, 2017.
5. Wieb Bosma, John Cannon, and Catherine Playoust. The Magma Algebra System I: The User Language. *Journal of Symbolic Computation*, 24(3):235–265, 1997.
6. 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.
7. Charles Bouillaguet, Pierre-Alain Fouque, and Gilles Macario-Rat. Practical key-recovery for all possible parameters of SFLASH. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, volume 7073 of *Lecture Notes in Computer Science*, pages 667–685. Springer, 2011.
8. Antoine Casanova, Jean-Charles Faugère, Gilles Macario-Rat, Jacques Patarin, Ludovic Perret, and Jocelyn Ryckeghem. GeMSS: A Great Multivariate Short Signature. Research report, UPMC - Paris 6 Sorbonne Universités ; INRIA Paris Research Centre, MAMBA Team, F-75012, Paris, France ; LIP6 - Laboratoire d'Informatique de Paris 6, December 2017.
9. Nicolas Courtois, Alexander Klimov, Jacques Patarin, and Adi Shamir. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 392–407. Springer, 2000.
10. Jintai Ding, Crystal Clough, and Roberto Araújo. Inverting square systems algebraically is exponential. *Finite Fields Their Appl.*, 26:32–48, 2014.
11. Jintai Ding, Joshua Deaton, Kurt Schmidt, Zheng Zhang, et al. Cryptanalysis of the lifted unbalanced oil vinegar signature scheme. In *Annual International Cryptology Conference*, pages 279–298. Springer, 2020.
12. Jintai Ding and Albrecht Petzoldt. Current state of multivariate cryptography. *IEEE Security & Privacy*, 15(4):28–36, 2017.
13. Jintai Ding and Dieter Schmidt. Rainbow, a new multivariable polynomial signature scheme. In John Ioannidis, Angelos D. Keromytis, and Moti Yung, editors, *Applied Cryptography and Network Security, Third International Conference, ACNS 2005, New York, NY, USA, June 7-10, 2005, Proceedings*, volume 3531 of *Lecture Notes in Computer Science*, pages 164–175, 2005.

14. Vivien Dubois, Pierre-Alain Fouque, Adi Shamir, and Jacques Stern. Practical cryptanalysis of SFLASH. In *Annual International Cryptology Conference*, pages 1–12. Springer, 2007.
15. Jean-Charles Faugère and Antoine Joux. Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using gröbner bases. In Dan Boneh, editor, *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, volume 2729 of *Lecture Notes in Computer Science*, pages 44–60. Springer, 2003.
16. Pierre-Alain Fouque, Louis Granboulan, and Jacques Stern. Differential cryptanalysis for multivariate schemes. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 341–353. Springer, 2005.
17. Aviad Kipnis and Adi Shamir. Cryptanalysis of the HFE public key cryptosystem by relinearization. In Michael J. Wiener, editor, *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, volume 1666 of *Lecture Notes in Computer Science*, pages 19–30. Springer, 1999.
18. Mingjie Liu, Lidong Han, and Xiaoyun Wang. On the equivalent keys in multivariate cryptosystems. *Tsinghua Science and Technology*, 16(3):225–232, 2011.
19. Gilles Macario-Rat and Jacques Patarin. Ariadne Thread and Pepper: New multivariate cryptographic schemes with public keys in degree 3. Cryptology ePrint Archive, Report 2021/084, 2021. `https://ia.cr/2021/084`.
20. Gilles Macario-Rat and Jacques Patarin. UOV-Pepper: New public key short signature in degree 3. Cryptology ePrint Archive, Report 2021/1006, 2021. `https://ia.cr/2021/1006`.
21. Tsutomu Matsumoto and Hideki Imai. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 419–453. Springer, 1988.
22. Jacques Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms. In Ueli M. Maurer, editor, *Advances in Cryptology - EUROCRYPT '96, International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, May 12-16, 1996, Proceeding*, volume 1070 of *Lecture Notes in Computer Science*, pages 33–48. Springer, 1996.
23. Jacques Patarin, Nicolas Courtois, and Louis Goubin. Quartz, 128-bit long digital signatures. In *Cryptographers' Track at the RSA Conference*, pages 282–297. Springer, 2001.
24. Jacques Patarin, Gilles Macario-Rat, Maxime Bros, and Eliane Koussa. Ultrashort multivariate public key signatures. *IACR Cryptol. ePrint Arch.*, 2020:914, 2020.
25. Daniel Smith-Tone. On the differential security of multivariate public key cryptosystems. In *International Workshop on Post-Quantum Cryptography*, pages 130–142. Springer, 2011.
26. Chengdong Tao, Albrecht Petzoldt, and Jintai Ding. Improved key recovery of the HFE$v-$ signature scheme. *IACR Cryptol. ePrint Arch.*, 2020:1424, 2020.