Practical Key-Recovery for All Possible Parameters of SFLASH

Charles Bouillaguet[1], Pierre-Alain Fouque[1], and Gilles Macario-Rat[2]

[1] École normale supérieure,
45 rue d'Ulm, 75005 Paris, France
{charles.bouillaguet,pierre-alain.fouque}@ens.fr
[2] Orange Labs
38–40, rue du Général Leclerc, 92794 Issy les Moulineaux Cedex 9, France
Gilles.Macariorat@orange-ftgroup.com

Abstract. In this paper we present a new practical key-recovery attack on the SFLASH signature scheme. SFLASH is a derivative of the older C* encryption and signature scheme that was broken in 1995 by Patarin. In SFLASH, the public key is truncated, and this simple countermeasure prevents Patarin's attack. The scheme is well-known for having been considered secure and selected in 2004 by the NESSIE project of the European Union to be standardized.

However, SFLASH was practically broken in 2007 by Dubois, Fouque, Stern and Shamir. Their attack breaks the original (and most relevant) parameters, but does not apply when more than half of the public key is truncated. It is therefore possible to choose parameters such that SFLASH is not broken by the existing attacks, although it is less efficient.

We show a key-recovery attack that breaks the full range of parameters in practice, as soon as the information-theoretically required amount of information is available from the public-key. The attack uses new cryptanalytic tools, most notably pencils of matrices and quadratic forms.

1 Introduction

Multivariate cryptography is a brand that encompasses the (mostly public-key) cryptographic schemes whose security relies on the difficulty of solving systems of multivariate polynomial equations over a finite field. Even when restricted to quadratic polynomials, and to the smallest possible finite field, the problem is well-known to be NP-complete, not to mention very difficult in practice. In that restricted setting, the problem is often called Multivariate Quadratic (MQ for short). Because this mathematical problem is well-known and has a simple statement, it was very tempting to design cryptographic schemes relying on its hardness. This has the added benefit that no quantum algorithm is known to break MQ faster than in the classical world, unlike most number-theoretic hard problem that would fall to Shor's algorithm [16].

Multivariate polynomials have been used in cryptography as early as in 1984, mostly with the purpose of designing RSA variants with faster decryption [11,12,5].

D.H. Lee and X. Wang (Eds.): ASIACRYPT 2011, LNCS 7073, pp. 667–685, 2011.

At about the same time, Matsumoto and Imai designed the first public-key scheme explicitly based on the hardness of MQ. In fact, they had several proposal, but only a single one (their "Scheme A") made it to the general crypto community, and was presented at Eurocrypt'88 [10] under the name C*. It is very similar to RSA, as its only non-linear component is a power function over a finite field. However, unlike RSA this power function is an easy-to-invert bijection, therefore in C* it is composed with two secret invertible linear maps that destroy its algebraic structure. We therefore see C* as an attempt to obfuscate a power function in $\mathbb{F}_{q^n}$ by presenting it as a collection of n quadratic polynomials in n variables over $\mathbb{F}_q$.

Several years later, Patarin found a devastating attack against C*, allowing to decrypt and to forge signatures in a few seconds [13]. He showed that there always are bilinear relations between the ciphertext and the plaintext, which can be easily discovered by the adversary. This allows for an efficient attack by substituting the ciphertext into the bilinear relations, which results in a system of linear equations whose solution is the plaintext.

The SFLASH signature scheme [14] is a derivative of the original C* that was proposed in 2001 by Courtois, Goubin and Patarin. It is famous for having been selected in 2003 by the NESSIE European project to be proposed to the standardization bodies.

The idea behind SFLASH is to take the original C* but to throw away a part of the output. The resulting trapdoor one-way function can no longer be used for encryption, but it can still be used for signatures. This is achieved by removing a part of the public key, which is the obfuscated description of the power function. The idea of removing some of the public polynomials has been originally suggested by Shamir [15], and was called the "Minus transform". The original C* with the minus transform is thus often called C*−. This countermeasure is very effective since it avoids the reconstruction of the bilinear relations and makes it much harder to compute Gröbner basis of the public key.

SFLASH has in turn been very badly broken in 2007 when Dubois, Fouque, Stern and Shamir found a practical forgery attack [4,3], and further broken in 2008 when Fouque, Macario-Rat and Stern found a practical key-recovery attack [6]. Both attacks are very practical, defeating the actual SFLASH parameters in minutes. They are essentially polynomial in the security parameter(s), so that there is no hope that increasing them may make the scheme simultaneously secure and usable.

However, both attacks only apply *as long as the number of removed polynomials is less than half of the total number*. There are therefore *unbroken* ranges of parameters, even though they are less practical than the original (defeated) proposal. For instance, let us consider the parameters $q = 128$ and $n = 257$. The original C* public key would be made of 257 polynomial in 257 variables over $\mathbb{F}_{128}$. If we throw away 75% of the public key, we obtain a C*− public-key with 64 multivariate quadratic polynomials in 257 variables, and the existing attacks do no apply. The signatures are 1799-bit long, and the public-key is 1.8Mbyte long. Forging a signature by exhaustive search requires 2^{448} trials, and computing a Gröbner basis should require even more arithmetic operations.

Our Contribution. We show that SFLASH/C^{*-} can be broken regardless of the fraction of the public that was thrown away, thus improving on the previous attacks. We present a practical key-only attack that recovers the secret-key and applies as soon as *three* polynomials from the public key are available. This happens to be the information-theoretic minimum quantity of data required to uniquely characterize the set of possible secret keys. The attack has been implemented and tested. It runs very efficiently, and breaks in practice all the meaningful ranges of parameters. For instance, the particular parameters mentioned in the previous paragraph can be broken in about 10 hours using a single computer.

SFLASH had already been thrown out of the league of possible alternatives to RSA of discrete-logarithm based schemes by the previous attacks. The contribution of this work is not only to further break SFLASH, but also to introduce new cryptanalytic techniques. To achieve our results, we make use of mathematical tools that were not previously used in multivariate cryptanalysis, such as pencils of matrices or quadratic forms, adjugate matrices, simultaneous diagonalization of quadratic forms, kernels of quadratic forms, etc. We expect that some of these tools might apply further to other schemes, in particular those sharing some features with SFLASH, notably HFE.

1.1 Organization of the Paper

In section 2, we present some mathematical background. Then, in section 3, we describe the C* and SFLASH signature schemes. In section 4, we investigate in great detail the mathematical properties of C* and find exploitable relations between the secret and public keys. Finally, we expose our key-recovery attack in section 5, and give experimental results.

2 Mathematical Background

Finite Fields. Let $\mathbb{K}$ the finite field with q elements, where q is a power of two, and $\mathbb{F}$ an extension of $\mathbb{K}$ of degree n. Recall that $\mathbb{F}$ is isomorphic to $\mathbb{K}^n$, so that we often identify the two spaces. The *trace* on $\mathbb{F}$ over $\mathbb{K}$ is the $\mathbb{K}$-linear map defined by $\mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(x) = x + x^q + \ldots + x^{q^{n-1}}$. The *norm* on $\mathbb{F}$ over $\mathbb{K}$ is defined by $\mathrm{N}_{\mathbb{F}/\mathbb{K}}(x) = x \cdot x^q \ldots \cdot x^{q^{n-1}}$. Both $\mathrm{Tr}_{\mathbb{F}/\mathbb{K}}$ and $\mathrm{N}_{\mathbb{F}/\mathbb{K}}$ are functions from $\mathbb{F}$ to $\mathbb{K}$, and we simply denote them Tr and N since there is no confusion. The map $x \mapsto x^q$ is called the Frobenius map, and it is a field automorphism.

Lemma 1. *For any $\mathbb{K}$-linear mapping L on $\mathbb{F}$ over $\mathbb{K}$, there exists an element λ of $\mathbb{F}$ such that, for all x in $\mathbb{F}$, $L(x) = \mathrm{Tr}(\lambda x)$. Moreover, if $\mathrm{Tr}(\lambda x) = 0$ for all $x \in \mathbb{F}$, then $\lambda = 0$.*

Quadratic forms. A quadratic form over $\mathbb{K}$ is a degree 2 homogeneous polynomial:

$$Q(x_1, \ldots, x_n) = \sum_{1 \le i \le j \le n} a_{ij} \cdot x_i x_j \quad \text{with } a_{ij} \in \mathbb{K}.$$

It is well-known that over fields of characteristic not two, a quadratic form Q is uniquely represented by its *polar form*, *i.e.*, the symmetric bilinear form defined by $\psi(Q) : (x, y) \mapsto 1/2 \cdot (Q(x + y) - Q(x) - Q(y))$, with the nice property that $Q(x) = \psi(Q)(x, x)$. Over fields of characteristic two, this is however no longer possible, because the division by two is not defined. In this paper, we will slightly abuse the usual definition, and we define the polar form of a quadratic form to be the symmetric bilinear form:

$$\psi(Q) : (x, y) \mapsto Q(x + y) - Q(x) - Q(y)$$

Given a basis $b_1, \ldots, b_n$ of $\mathbb{F}$, $\psi(Q)$ can be represented by a $n \times n$ symmetric matrix whose (i, j) coefficient is $\psi(Q)\,(b_i, b_j)$. By an abuse of notation, we will often identify $\psi(Q)$ with its matrix representation.

The Kernel of a Quadratic Form. The *kernel* of a quadratic form Q, also called the *radical* of Q is the vector space of elements $a \in \mathbb{F}$ such that for any $x \in \mathbb{F}$, $\psi(Q)(x, a) = 0$. It is easy to see that the kernel of a quadratic form is the kernel of the matrix $\psi(Q)$. What makes the kernel interesting is that in characteristic two, when n is odd, all quadratic forms have a non-trivial kernel.

Theorem 1 ([1]). *Let q be a power of two, and let Q be a quadratic form over $\mathbb{K}$. Then the rank of $\psi(Q)$ is even.*

Linear Algebra. We denote the characteristic polynomial of M by $\chi\,(M)$. A *minor* of M is simply the determinant of a submatrix of M. We will use in the following the *adjugate* matrix $\mathrm{adj}(M)$ of a matrix M. We recall that it is the transpose of the comatrix, which is the matrix of the cofactors. A cofactor of M, $\mathrm{cof}_{i,j}(M)$ is the determinant of the submatrix $M_{\overline{i}}^{\overline{j}}$, where in this notation we refer to the matrix M without the ith row and the jth column. We lastly recall two well-known results connecting a matrix M and its adjugate.

Theorem 2 (Cayley-Hamilton). *If $\chi\,(M) = X^n + c_{n-1}X^{n-1} + \cdots + c_1X + c_0$ is the* characteristic polynomial *of M, then:*

$$M^n + c_{n-1}M^{n-1} + \cdots + c_1M + c_0 \cdot I_n = 0$$
$$M^{n-1} + c_{n-1}M^{n-2} + \cdots + c_2M + c_1 \cdot I_n = \mathrm{adj}(-M)$$

It follows that $-M \cdot \mathrm{adj}(-M) = \mathrm{adj}(-M) \cdot -M = \det(-M) \cdot I_n$

Lemma 2. *The rank of* $\mathrm{adj}(M)$ *can be deduced from the rank of M:*

- *if* $\mathrm{rank}(M) = n$, *then* $\mathrm{rank}(\mathrm{adj}(M)) = n$.
- *if* $\mathrm{rank}(M) = n - 1$, $\mathrm{rank}(\mathrm{adj}(M)) = 1$.
- *In all other cases,* $\mathrm{rank}(\mathrm{adj}(M)) = 0$.

3 The C* and SFLASH Signature Schemes

The basic idea underlying both C* and SFLASH is to hide an easily invertible function ϕ in the large finite field $\mathbb{F}$ using two secret invertible linear (or affine) maps S and T which mix together the n coordinates of ϕ over the small field $\mathbb{K}$, with $\mathbf{PK} = T \circ \phi \circ S$. The signature of a message y is a vector x such that $\mathbf{PK}(x) = y$. The legitimate signer easily computes x by successively inverting T, ϕ and then S.

Let π be the canonical isomorphism between $\mathbb{K}^n$ and $\mathbb{F}$, and let ϕ be defined by $\phi(X) = X^{1+q^\theta}$. Enforcing that $\gcd(1+q^\theta, q^n-1) = 1$ makes ϕ bijective. Because we may write $\phi(X) = X \cdot X^{q^\theta}$, we find that ϕ is in fact the product of two linear functions (recall that the Frobenius map and its iterates are linear). It follows that $\pi \circ \phi \circ \pi^{-1}$ is a quadratic bijection of $\mathbb{K}^n$, *i.e.*, that if $x \in \mathbb{K}^n$, then $\pi \circ \phi \circ \pi^{-1}$ is a vector whose coordinates are quadratic forms in the coordinates of x. For the sake of lighter notations, we omit π in the sequel.

The secret key of the scheme is composed by the two invertible $n \times n$ matrices S and T with coefficients in $\mathbb{K}$. The exponent θ and π are public parameters. The public-key of the scheme is formed by the representation over $\mathbb{K}^n$ of $T \circ \phi \circ S$. More precisely, if T_i denotes the i-th line of T, then the public key of C^* is the vector of n quadratic forms over $\mathbb{K}^n$:

$$\mathcal{P}_i(x_1, \ldots, x_n) = \mathrm{Tr}\Big(T_i \cdot \phi\left(S(x_1, \ldots, x_n)\right)\Big) \quad 1 \le i \le n$$

The public key of SFLASH is composed of the first r quadratic forms $\mathcal{P}_1, \ldots, \mathcal{P}_r$. Typical values of the parameter may be the ones defined for SFLASH V3: $q = 128, n = 67, r = 56$ and $\theta = 33$.

Although the public key is a vector of polynomials in $(\mathbb{K}[x_1, \ldots, x_n])^n$, it is more convenient to see them as functions from $\mathbb{F}$ to $\mathbb{K}$. We therefore write

$$\mathcal{P}_i(x) = \mathrm{Tr}\left(T_i \cdot S(x)^{1+q^\theta}\right).$$

Equivalent Secret Keys. Given a public-key, there are many possible corresponding secret keys (there are "equivalent" secret keys [18]). A key-recovery attack is expected to retrieve one possible secret key amongst those generating the targeted public-key. The existence of many equivalent secret keys gives some freedom to the attacker: we may be guaranteed that there is an equivalent secret key satisfying some interesting property.

Lemma 3. *If (S, T) is an SFLASH secret-key that generates the public key $\mathbf{PK}$, then for any integer $k > 1$ there is an equivalent secret key (S', T') in which $T'_i = (T_i/T_1)^{q^k}$ (seeing the vectors T_i as elements of $\mathbb{F}$).*

Proof. Because the function $x \in \mathbb{F} \mapsto a \cdot x$ is linear over $\mathbb{F}$, it can be represented by a matrix M_a over $\mathbb{K}^n$. The key idea is that multiplications "commute" with the internal power function:

$$\mathcal{P}_i(x) = \mathrm{Tr}\left(\frac{T_i}{a^{1+q^\theta}} \cdot [a \times (S \cdot x)]^{1+q^\theta}\right)$$

Now, we pick a such that $a^{1+q^\theta} = T_1$ (this is always possible because the power function is bijective). Thus, a possible equivalent secret key is such that $T'_i = T_i/T_1$, and $S' = M_a \cdot S$.

Next, it follows from the definition of the trace, and from the identity $x^{q^n} = x$ which holds over $\mathbb{F}$ that $\mathrm{Tr}\left(x^{q^k}\right) = \mathrm{Tr}(x)$. This shows that

$$\mathcal{P}_i(x) = \mathrm{Tr}\left(\left(\frac{T_i}{a^{1+q^\theta}}\right)^{q^k} \cdot \left([(a \times (S \cdot x)]^{q^k}\right)^{1+q^\theta}\right)$$

Thus, if F denotes the matrix representing the Frobenius, *i.e.*, the linear map $x \mapsto x^q$ in $\mathbb{F}$, then a possible equivalent secret key is such that $T'_i = (T_i/T_1)^{q^k}$, and $S' = F^k \cdot M_a \cdot S$. □

4 Mathematical Properties of C*− Public Keys

The aim of this section is to exhibit relations involving the secret elements S and the T_i's on the one hand, and the public key on the other hand, in such a way that the secrets can be easily reconstructed given only a small number of public polynomials.

For this purpose, we consider two public polynomials $\mathcal{P}_i$ and $\mathcal{P}_j$, and we define the *pencil of quadratic forms* $\mathbf{P} = \lambda\mathcal{P}_i + \mu\mathcal{P}_j$, with λ, μ in $\mathbb{K}$. We also define the *pencil of vectors* $\mathbf{T} = \lambda T_i + \mu T_j$, and because the Trace is $\mathbb{K}$-linear we have:

$$\mathbf{P}(X) = \mathrm{Tr}\left(\mathbf{T} \cdot S(X)^{1+q^\theta}\right). \tag{1}$$

We are interested in the *kernel* of $\mathbf{P}$, which is by definition the set of vectors a such that for any x, $\psi(\mathbf{P})(a, x) = 0$. In fact, it is simply the kernel of the matrix representation of the polar form $\psi(\mathbf{P})$. We first relate the kernel of $\mathbf{P}$ to the components of the secret key in section 4.1, and then with the components of the public-key in section 4.2. This allows us, by "transitivity", to find exploitable relations between the public key and the secret elements in section 4.3.

In the sequel, we adopt the typographic convention that any quantity that depends implicitly on λ and μ is written in bold.

4.1 Relations between the Kernel and the Secret-Key

It is not very surprising that the kernel of $\mathbf{P}$ admits a relatively simple expression in terms of the components of the secret key.

Theorem 3. *Given that n is odd, and $gcd(\theta, n) = 1$, we have:*

(*i*) *The kernel of* $\mathbf{P}$ *is* $\left\{x \in \mathbb{K}^n \mid \mathbf{T} \cdot S(x)^{1+q^\theta} \in \mathbb{K}\right\}$.
(*ii*) *The matrix pencil* $\psi(\mathbf{P})$ *has rank* $n - 1$.
(*iii*) *When* $(\lambda, \mu) \neq (0, 0)$, *there exists a unique vector* $\mathbf{a} \in \mathbb{K}^n$ *in the kernel of* $\mathbf{P}$ *such that* $\mathbf{P}(\mathbf{a}) = 1$.

(*iv*) *There exists* $\delta \in \mathbb{N}$ *such that* $\mathbf{a} = S^{-1}\left(\mathbf{T}^{\delta}\right)$. *A possible value for* δ *is*

$$\delta = \left(\frac{q}{2} - 1\right) \cdot \sum_{i=0}^{n-1} q^i + \sum_{i=(n+1)/2}^{n-1} q^{2i\theta} \tag{2}$$

Proof. It is known that the polar forms of C* polynomials have a special shape:

$$\psi(\mathbf{P})(x, y) = \mathrm{Tr}\left(\mathbf{T} \cdot \left[S(x) \cdot S(y)^{q^\theta} + S(x)^{q^\theta} \cdot S(y)\right]\right)$$

After some manipulations, by exploiting the linearity of the Frobenius, of the Trace, and the fact that they commute, we find when $x \neq 0$:

$$\psi(\mathbf{P})(x, y) = \mathrm{Tr}\left(\left[\mathbf{T} \cdot S(x)^{1+q^\theta} + \left(\mathbf{T} \cdot S(x)^{1+q^\theta}\right)^{q^\theta}\right] \cdot \left(\frac{S(y)}{S(x)}\right)^{q^\theta}\right)$$

Now, inside the trace, the first term of the product depends only on x, and the second member takes all possible values in $\mathbb{F}$ when y ranges across $\mathbb{F}$, because S and the Frobenius are bijective. Lemma 1 then tells us that if $x \neq 0$ belongs to the kernel of $\mathbf{P}$, then

$$\mathbf{T} \cdot S(w)^{1+q^\theta} + \left(\mathbf{T} \cdot S(w)^{1+q^\theta}\right)^{q^\theta} = 0$$

It remains to show that the solutions of the equation $X + X^{q^\theta} = 0$ in $\mathbb{F}$ are precisely the elements of $\mathbb{K}$. It is easy to check that any $x \in \mathbb{K}$ is a solution, because the fields are of characteristic two, which makes the equation equivalent to $X = X^{q^\theta}$. The other direction is not much more difficult: by induction we find that $X = X^{q^{i\theta}}$ for any $i \in \mathbb{N}$. Since over $\mathbb{F}$ we always have $x = x^{q^n}$, then when $i\theta$ is congruent to 1 modulo n, the equation implies $X + X^q = 0$, which shows that the solutions all lies in $\mathbb{K}$. This establishes point (*i*).

Let us prove point (*ii*). The polar form $\psi(\mathbf{P})$ cannot be of rank n, because it is a skew-symmetric matrix and n is odd (this is well-known for matrices over fields, and is extended to the case of matrices multivariate polynomial rings in lemma 8, appendix A). Now, we show that the rank of $\psi(\mathbf{P})$ is greater than $n-1$. If we specialize (λ, μ) to any value in $\mathbb{K}^2$ distinct from $(0, 0)$, then by point (*i*) $\psi(\lambda\mathcal{P}_i + \mu\mathcal{P}_j)$, seen as a matrix with entries in $\mathbb{K}$, has a kernel of dimension 1. By the rank theorem (over $\mathbb{K}$), its rank is then $n - 1$. This shows that there is a non-zero minor of dimension $(n - 1)$. This minor (seen as a polynomial in λ and μ) cannot be the zero polynomial, otherwise it could become non-zero for a particular choice of λ and μ in $\mathbb{K}$, hence the rank of $\psi(\mathbf{P})$ (seen as a matrix with entries in $\mathbb{K}[\lambda, \mu]$ has rank exactly $n - 1$.

Point (*iii*) follows immediately from (*i*) and from the fact S, T and the power function are bijective. To establish point (*iv*), we need to find a suitable value δ such that $S(a) = \mathbf{T}^{\delta}$. By definition of a, we should have $\left(\mathbf{T}^{\delta}\right)^{1+q^\theta} \cdot \mathbf{T} = 1$, so that δ satisfies the equation $1 + \delta(1 + q^\theta) = 0$ modulo $(q^n - 1)$. Checking that the given value of δ is valid is technical and not very interesting, and we refer the reader to [8] for more details. □

The fourth point of theorem 3 makes it possible to explicitly write down the expression of $\mathbf{a}$, the kernel vector introduced in the proposition, as a function of λ and μ. Let us set $d = (n-1)/2$, and let us introduce $P_N, P_S \in \mathbb{F}[\lambda, \mu]$:

$$p_N = \mathrm{N}(\mathbf{T}) = \prod_{i=0}^{n-1} \left(\lambda \cdot {T_1}^{q^i} + \mu \cdot {T_2}^{q^i}\right)$$

$$p_S = S^{-1}\left(\prod_{i=(n+1)/2}^{n-1} \left(\lambda \cdot {T_1}^{q^{2i\theta}} + \mu \cdot {T_2}^{q^{2i\theta}}\right)\right) \tag{3}$$

The idea is that p_N only depends on T, while p_S depends "linearly" on S. It is fairly obvious that p_N has total degree n while p_S has total degree d. Next, we claim that p_N in fact has coefficients in $\mathbb{K}$. A possible way to see this is that because it coincides with the Norm, it takes values in $\mathbb{K}$ when $\lambda, \mu \in \mathbb{K}$, and therefore it could be interpolated as a polynomial of $\mathbb{K}[\lambda, \mu]$.

We have carefully chosen p_N and p_S so that the vector $\mathbf{a}$ defined in point (*iii*) of proposition 3 is such that:

$$\mathbf{a} = (p_N)^{q/2-1} \cdot p_S.$$

This fact is an easy consequence of the fourth point of proposition 3. Note that because p_N has values in $\mathbb{K}$, then $p_S(\lambda, \mu)$ spans the kernel of $\mathbf{P}$, but unlike $\mathbf{a}$, p_S does not *a priori* satisfy the additional condition that $\mathbf{P}(p_S) = 1$. It follows, by definition of $\mathbf{a}$, because $\mathbf{P}(\lambda x) = \lambda^2 \mathbf{P}(x)$ when $\lambda \in \mathbb{K}$ and because $x^{-1} = x^{q-2}$ in $\mathbb{K}$, that:

$$\mathbf{P}\left((p_N)^{q/2-1} \cdot p_S\right) = \frac{\mathbf{P}(p_S)}{p_N} = 1$$

And we find that $p_N = \mathbf{P}(p_S)$. The two polynomials p_N and p_S play a crucial role in the sequel: we will show in section 5 that knowing them is sufficient to reconstruct the secret key in polynomial time. In addition, we will also show that they can be reconstructed in polynomial time from the public-key. However, doing this requires some more mathematical machinery.

4.2 Relations between the Kernel and the Public Key

The kernel of $\mathbf{P}$ can be computed using only publicly available information, since it only depends on the public polynomials. If the values of λ and μ were fixed, this could be achieved with standard linear algebra. More sophisticated computer algebra systems have functions that compute a basis of the kernel in terms of λ and μ. We remove the need for such sophisticated operations by explicitly giving the form of the kernel.

Theorem 4. *Let* $\mathbf{P}$ *be a pencil of two public polynomials,* $B = \{b_1, \ldots, b_n\}$ *a basis of* $\mathbb{K}^n$*. There exists a vector* $\mathbf{k} = (\mathbf{k}_1, \ldots, \mathbf{k}_n)$ *of degree-d homogeneous bivariate polynomials in* $\mathbb{K}[\lambda, \mu]$*, such that:*

i) The adjugate matrix of the polar form of $\mathbf{P}$ *can be expressed as the tensor product of* $\mathbf{k}$ *with itself:*

$$adj\left(\psi(\mathbf{P})\right) = \left(\mathbf{k}_i \cdot \mathbf{k}_j\right)_{1 \leq i,j \leq n}$$

ii) the kernel of $\psi(\mathbf{P})$ *is spanned by* $\sum_{i=1}^{n} \mathbf{k}_i \cdot b_i$

Proof. According to theorem 3, item (ii), the matrix pencil $\psi(\mathbf{P})$ is of rank $n-1$, and lemma 2 states that in this case $\mathrm{adj}(\psi(\mathbf{P}))$ has rank 1. We will now show that $\mathrm{adj}(\psi(\mathbf{P}))$ is the square of some other matrix, but we first require a technical lemma.

Lemma 4. *Let* $\mathbf{P}$ *be an arbitrary pencil of quadratic forms. There exists a family of bivariate polynomials* $\mathbf{p}_0, \ldots, \mathbf{p}_d \in \mathbb{K}[\lambda, \mu]$ *such that* $\mathbf{p}_i$ *is homogeneous of degree* i*, and the characteristic polynomial of the polar form of* $\mathbf{P}$ *is:*

$$\chi\left(\psi\left(\mathbf{P}\right)\right) = \sum_{i=0}^{d} {\mathbf{p}_i}^2 \cdot X^{n-2i}.$$

The proof of lemma 4 is postponed to appendix A. It follows from lemma 4 and theorem 2 that:

$$\mathrm{adj}(\psi(\mathbf{P})) = \sum_{i=0}^{d} {\mathbf{p}_i}^2 \cdot \psi(\mathbf{P})^{2d-2i} = \left(\sum_{i=0}^{d} \mathbf{p}_i \cdot \psi(\mathbf{P})^{d-i}\right)^2.$$

We denote by R the natural square-root of $\mathrm{adj}(\psi(\mathbf{P}))$ occurring on the right-hand side. It is a symmetric matrix pencil whose coefficients are bivariate polynomials of degree d in λ and μ. Let us consider the i-th diagonal term of $\mathrm{adj}(\psi(\mathbf{P}))$. We find:

$$\mathrm{adj}(\psi(\mathbf{P}))_{i,i} = \sum_{j=1}^{n} R_{i,j} \cdot R_{j,i} = \left(\sum_{j=1}^{n} R_{i,j}\right)^2.$$

Consequently, let us define $\mathbf{k}_i = \sum_{j=1}^{n} R_{i,j}$. The previous equation tells us that $\mathrm{adj}(\psi(\mathbf{P}))_{i,i} = {\mathbf{k}_i}^2$ for all $1 \leq i \leq n$. This establishes point (i) for the diagonal of $\mathrm{adj}(\psi(\mathbf{P}))$ only.

Let us now consider the other terms with $i \neq j$. Since $\mathrm{adj}(\psi(\mathbf{P}))$ is of rank 1, we know that all the minors of dimension 2 of $\mathrm{adj}(\psi(\mathbf{P}))$ obtained by keeping only the i-th row and the j-th column is null. This yields:

$$\mathrm{adj}(\psi(\mathbf{P}))_{i,i} \cdot \mathrm{adj}(\psi(\mathbf{P}))_{j,j} + \left(\mathrm{adj}(\psi(\mathbf{P}))_{i,j}\right)^2 = 0$$

and consequently $\mathrm{adj}(\psi(\mathbf{P}))_{i,j} = \mathbf{k}_i \cdot \mathbf{k}_j$ (when the field is of characteristic two, the square root always exists and is unique because the Frobenius map is bijective). This completes the proof of (i).

Let us now focus on point (*ii*). One of the $\mathbf{k}_i$'s at least is non-zero, because $\mathrm{adj}(\psi(\mathbf{P}))$ is not the null matrix. We therefore assume (without loss of generality) that $\mathbf{k}_1$ is non-zero, and we consider the matrix relation given by theorem 2:

$$\psi(\mathbf{P}) \cdot \mathrm{adj}(\psi(\mathbf{P})) = 0.$$

Looking at the first column of the product, we conclude that

$$\psi(\mathbf{P}) \cdot \left(\sum_{i=1}^{n} \mathbf{k}_1 \mathbf{k}_i \cdot b_i \right) = 0,$$

and because $\mathbf{k}_1$ is non-zero, we conclude that $\psi(\mathbf{P}) \cdot (\sum_{i=1}^{n} \mathbf{k}_i \cdot b_i) = 0$. □

In light of theorem 4, it seems that we can derive from the public key a polynomial whose properties mimic those of p_S. Keeping the notations of the theorem, we define:

$$\widetilde{p}_S = \sum_{i=1}^{n} \mathbf{k}_i \cdot b_i, \qquad \widetilde{p}_N = \mathbf{P}\left(\widetilde{p}_S\right)$$

We deduce from theorem 4 that $\widetilde{p}_S$ has the same degree as p_S, and that like p_S, it spans the kernel of $\psi(\mathbf{P})$. We also need to find a polynomial $\widetilde{p}_N$ that would be an analogous of p_N and that could be derived from the public key. Note that it immediately follows from theorem 4 that $\widetilde{p}_S$ spans the kernel of $\mathbf{P}$.

4.3 Relations between the Secret-Key and the Public-Key

The last (but not least) step of our analysis is to show that the two polynomials p_N, p_S derived from the secret key in section 4.1 on the one hand, and the polynomials $\widetilde{p}_N, \widetilde{p}_S$ derived from the public key in section 4.2 are in general equal up to a constant multiplicative factor.

Theorem 5. *If T_2/T_1 is primitive over $\mathbb{F}$ (i.e., generates the multiplicative group of $\mathbb{F}$), then there exists a constant $\zeta \neq 0$ in $\mathbb{K}$ such that $\widetilde{p}_S = \zeta \cdot p_S$, and (accordingly) $\widetilde{p}_N = \zeta^2 \cdot p_N$.*

Proof. The first step of the proof is to show that $\widetilde{p}_N$ has degree n, just like p_N. The polynomials $\mathbf{k}_1, \ldots, \mathbf{k_n}$ defined in theorem 4 have coefficients in $\mathbb{K}$, and are homogeneous of degree d. We can therefore find a family $c_0, \ldots, c_d$ of coefficients in $\mathbb{F}$ such that:

$$\widetilde{p}_S = \sum_{i=1}^{n} \mathbf{k}_i \cdot b_i = \sum_{i=0}^{d} c_i \cdot \lambda^{d-i} \mu^i. \tag{4}$$

It turns out that this family enjoys a nice property: over the subspace of $\mathbb{K}^n$ that it spans, the pencil $\mathbf{P}$ is in fact a diagonal form (*i.e.*, the two public polynomial it is made of are simultaneously diagonal).

Lemma 5. *$\psi(\mathbf{P})(c_i, c_j) = 0$ for any $0 \leq i, j \leq d$.*

Lemma 6. *For any family* $\{r_i\}_{0\leq i\leq d}$ *of polynomials over* $\mathbb{K}$*, we have*

$$\mathbf{P}\left(\sum_{i=0}^{d} r_i \cdot c_i\right) = \sum_{i=0}^{d} r_i^2 \cdot \mathbf{P}(c_i).$$

The proofs are postponed to appendix B. Applying lemma 6 to (4), we get:

$$\widetilde{p}_N = \mathbf{P}\left(\widetilde{p}_S\right) = \mathbf{P}\left(\sum_{i=0}^{d} c_i \cdot \lambda^{d-i}\mu^i\right) = \sum_{i=0}^{d}\Big(\lambda\mathcal{P}_1(c_i) + \mu\mathcal{P}_2(c_i)\Big) \cdot \lambda^{2d-2i}\mu^{2i}$$

From there, it is easy to see that $\widetilde{p}_N$ has degree $2d+1 = n$.

Now that it has been established that p_N and $\widetilde{p}_N$ have the same degree, we will use irreducibility properties of p_N to conclude the proof of theorem 5. We first claim that the univariate polynomial $p_N(\lambda, 1) \in \mathbb{K}[\lambda]$ is irreducible over $\mathbb{K}$. After a few manipulations we find

$$p_N(\lambda, 1) = \mathrm{N}(\lambda T_1 + T_2) = \mathrm{N}(T_1) \cdot \mathrm{N}(\lambda + T_2/T_1).$$

Thus T_2/T_1, which is primitive over $\mathbb{F}$, is a root of $p_N(\lambda, 1)$, and this polynomial is therefore irreducible over $\mathbb{K}$.

Lemma 7. *There exist* $\zeta, \widetilde{\zeta}$ *in* $\mathbb{K}[\lambda, \mu]$ *such that:*

$$\zeta \cdot p_S = \widetilde{\zeta} \cdot \widetilde{p}_S \quad \textit{and} \quad \gcd\left(\zeta, \widetilde{\zeta}\right) = 1.$$

Proof. First, the rank of the two-column matrix $(p_S, \widetilde{p}_S)$ is one. If it was two, then this matrix could be extended to a $n \times n$ matrix M of rank n. We then find that the rank of $\psi(\mathbf{P}) \cdot M$ would be at most $n-2$, since its two first columns are null, which contradicts the fact established earlier that $\psi(\mathbf{P})$ has rank $n-1$.

There exist polynomials $\{\ell_i\}$ such that $p_S = \sum_{i=1}^{n} \ell_i \cdot b_i$. We now argue that there exists an index i_0 such that $\mathbf{k}_{i_0} \neq 0$ and $\ell_{i_0} \neq 0$. The reasoning is by contradiction: assume that for all i we have $\mathbf{k}_i \cdot \ell_i = 0$. Since $\widetilde{p}_S \neq 0$ and $p_S \neq 0$, there exist indices i, j such that $\mathbf{k}_i \neq 0$ and $\ell_j \neq 0$. By hypothesis, $\mathbf{k}_j = 0$ and $\ell_i = 0$. But then, we find that $\mathbf{k}_i \cdot \ell_j + \mathbf{k}_j \cdot \ell_i = \mathbf{k}_i \cdot \ell_j \neq 0$. Consequently, a minor of dimension two of $(p_S, \widetilde{p}_S)$ is non-zero, which contradict the fact that it is of rank one.

We can therefore assume without loss of generality that $\mathbf{k}_1 \neq 0$ and $\ell_1 \neq 0$. The linear combination $\mathbf{k}_1 \cdot p_S + \ell_1 \cdot \widetilde{p}_S$ is null since by construction its first coordinate is zero, and the other coordinates are minors of dimension 2 of $(p_S, \widetilde{p}_S)$ and are also null. We can now assert that the pair

$$\left(\frac{\mathbf{k}_1}{\gcd(\mathbf{k}_1, \ell_1)}, \frac{\ell_1}{\gcd(\mathbf{k}_1, \ell_1)}\right)$$

satisfies the requirements of the lemma. □

Let $\left(\zeta, \widetilde{\zeta}\right)$ a pair of bivariate polynomials over $\mathbb{K}$ satisfying lemma 7. By applying $\mathbf{P}$, we get: $\zeta^2 \cdot p_N = \widetilde{\zeta}^2 \cdot \widetilde{p}_N$. Any irreducible factor of $\widetilde{\zeta}$ must divide p_N since it does not divide ζ. But because p_N is irreducible, $\widetilde{\zeta}$ is necessarily of degree 0. And ζ is also degree 0 because p_N and $\widetilde{p_N}$ have the same degree. This concludes the proof of theorem 5. □

We conclude this section by giving one last important but somewhat technical result. The polynomial p_S is "designed" to reveal the image of S on the subspace of $\mathbb{K}^n$ spanned by its $d+1$ coefficients (seen as vectors of $\mathbb{K}^n$). It does actually matter whether these are linearly independent or not.

Theorem 6. *The coefficients of the polynomials p_S form an independent family if and only if $(T_2/T_1)^{q^\theta}$ is not a root of the polynomials $x+x^{q^{2i\theta}}$ for $1 \leq i \leq d$. In particular, if n is a prime number this condition is satisfied since by assumption T_1 and T_2 are independent.*

The proof is given in appendix C.

5 The Attack

We are now ready to leverage our in-depth investigation of the properties of C*, by presenting a practical key-recovery attack that does not require any signature. The global attack strategy is to compute the polynomials $\widetilde{p}_N$ and $\widetilde{p}_S$ defined in section 4.2. Then, theorem 5 tells us that with non-negligible probability, these are equal to the polynomials p_N and p_S defined in section 4.1, from which the secret-key can be efficiently recovered.

Reconstructing the Polynomials p_N and p_S. Given a pencil $\mathbf{P} = \lambda\mathcal{P}_i + \mu\mathcal{P}_j$ of polynomials from the public key, we first show how the polynomials $\widetilde{p}_N$ and $\widetilde{p}_S$ defined in section 4.2 can be determined. More precisely, we show how to build a function Kernel-Recovery($\mathbf{P}$) that returns the two polynomials p_N and p_S described in section 4.1. Because $p_N = \mathbf{P}(p_S)$, we focus our attention on the non-obvious part consisting in recovering p_S. This can be achieved in two different ways. A first possibility is to follow the proof of theorem 4, which results in the following procedure:

1. Compute the characteristic polynomial ζ of $\psi(\mathbf{P})$ and factor it into
$$\zeta = X \cdot \left(\sum_{i=0}^{d} {\mathbf{p}_i}^2 \cdot X^{d-i} \right)^2$$
2. Compute the matrix $\mathbf{R} = \sum_{i=0}^{d} \mathbf{p}_i \cdot \psi(\mathbf{P})^{d-i}$ and let $\mathbf{k}_i = \sum_{j=1}^{n} \mathbf{R}_{i,j}$.
3. Finally let p_S be equal to $\sum_{i=1}^{n} \mathbf{k}_i \cdot b_i$

Note that computing the characteristic polynomial can be achieved over any commutative ring using the division-free algorithm of Mahajan and Vinay [9]. Computing the factorization of the characteristic polynomial is a (classical) multivariate factorization problem. Both functionality are available in several computer algebra systems, including (but not limited to) MAGMA [2] and SAGE [17].

Alternatively, we may directly compute a basis of $\ker \psi(\mathbf{P})$ (which is a module over $\mathbb{K}[\lambda, \mu]$) using the *ad hoc* function present in some computer algebra systems. This function is for instance available in MAGMA, and seems to rely on Gröbner basis computations. It is apparently much faster than the previous option.

From Kernel to Secret-Key. Let us call (T', S') the equivalent key we try to forge. Thanks to lemma 3, we know that we may without loss of generality assume that $T'_1 = 1$ and $T'_2 = (T_2/T_1)^{q^i}$, for any $i > 0$. This shows that if $(p_N, p_S) = \text{KERNEL-RECOVERY}(\lambda\mathcal{P}_1 + \mu\mathcal{P}_2)$, then we may safely choose T'_2 to be any root of $p_N(\lambda, 1)$ different from one. We then focus on equation (3):

$$p_S = S^{-1}\left(\prod_{i=(n+1)/2}^{n-1}\left(\lambda \cdot {T_1}^{q^{2i\theta}} + \mu \cdot {T_2}^{q^{2i\theta}}\right)\right)$$

Given the values of T'_1 and T'_2, we may explicitly evaluate the product on the right-hand side. Identifying both sides coefficient-wise then reveals the image of S' on the subspace of K^n spanned by the $d+1$ coefficients of the product. Theorem 6 tells us that this subspace is of dimension $d+1$ with non-negligible probability.

To complete the key-recovery of the secret element, we use a third polynomial from the public-key. We compute $(p'_N, p'_S) = \text{KERNEL-RECOVERY}(\lambda\mathcal{P}_1 + \mu\mathcal{P}_3)$. Only one of the roots of p'_N yields a valid choice for T'_3, therefore we pick one at random, and we will try again with another one in case of failure in the subsequent steps. Knowledge of T'_1 and T'_3 allows to discover the image of S' on another subspace spanned by $d+1$ generators following the same procedure.

At this point, we have learned the image of S' on $n+1$ vectors, and we really hope that S' is completely revealed. If it is not the case, we may try again with $\mathcal{P}_4$ instead of $\mathcal{P}_3$. Once S' is known, finding the other T_i's can be done by straightforward linear algebra. If no solution exists for any of them, then our guess for T'_3 was wrong.

5.1 Complexity

We implemented the whole key-recovery using the MAGMA computer algebra system. The code of the full attack is 120 lines long, and is available on the web page of the first author. We first applied the attack to SFLASH v2 and SFLASH v3, that were already broken (universal forgery) by Dubois, Fouque, Stern and Shamir [3], and further broken (key-recovery) by Fouque, Macario-Rat and Stern [6]. We then applied the attack to SFLASH instances that cannot be broken by the existing attack, because the number of polynomials in the public

Table 1. Experimental results

SFLASH version	q	n	#public polynomials	Signature size	Already broken ?	Attack time	KeyGen time
v2	128	37	26 (70%)	259 bits	[3,6]	7s	0.1s
v3	128	67	56 (83%)	469 bits	[3,6]	47s	0.6s
	256	131	56 (42%)	1048 bits	No	17min	5s
	65536	257	64 (25%)	4112 bits	No	$\approx$ 10h	141s
	2	331	80 (24%)	331 bits	No	105min	16s
	2	521	80 (24%)	521 bits	No	$\approx$ 11h	62s
	2	1031	128 (12%)	1031 bits	No	...	680s

key is less than $n/2$. We tried various combinations of field size and variable numbers, and found out that the attack works quite well in practice, as Table 1 shows. There are thus no longer any practically unbroken set of parameters for SFLASH.

References

1. Albert, A.A.: Symmetric and alternate matrices in an arbitrary field, i. Transactions of the American Mathematical Society 43(3), 386–436 (1938)
2. Bosma, W., Cannon, J.J., Playoust, C.: The Magma Algebra System I: The User Language. J. Symb. Comput. 24(3/4), 235–265 (1997)
3. Dubois, V., Fouque, P.A., Shamir, A., Stern, J.: Practical Cryptanalysis of SFLASH. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 1–12. Springer, Heidelberg (2007)
4. Dubois, V., Fouque, P.A., Stern, J.: Cryptanalysis of SFLASH with Slightly Modified Parameters. In: Naor, M. (ed.) EUROCRYPT 2007. LNCS, vol. 4515, pp. 264–275. Springer, Heidelberg (2007)
5. Fell, H.J., Diffie, W.: Analysis of a Public Key Approach Based on Polynomial Substitution. In: Williams, H.C. (ed.) CRYPTO 1985. LNCS, vol. 218, pp. 340–349. Springer, Heidelberg (1986)
6. Fouque, P.A., Macario-Rat, G., Stern, J.: Key Recovery on Hidden Monomial Multivariate Schemes. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 19–30. Springer, Heidelberg (2008)
7. Lidl, R., Niederreiter, H.: Finite Fields. Cambridge University Press (2008)
8. Macario-Rat, G.: Cryptanalyse de schémas multivariés et résolution du problème Isomorphisme de Polynômes. PhD thesis, Université Paris Diderot — Paris 7 (June 2010)
9. Mahajan, M., Vinay, V.: Determinant: Combinatorics, algorithms, and complexity. Chicago J. Theor. Comput. Sci. 1997 (1997)
10. Matsumoto, T., Imai, H.: Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption. In: Günther, C.G. (ed.) EUROCRYPT 1988. LNCS, vol. 330, pp. 419–453. Springer, Heidelberg (1988)
11. Ong, H., Schnorr, C.P., Shamir, A.: An efficient signature scheme based on quadratic equations. In: STOC, pp. 208–216. ACM (1984)

12. Ong, H., Schnorr, C.P., Shamir, A.: Efficient Signature Schemes Based on Polynomial Equations. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 37–46. Springer, Heidelberg (1985)
13. Patarin, J.: Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt '88. In: Coppersmith, D. (ed.) CRYPTO 1995. LNCS, vol. 963, pp. 248–261. Springer, Heidelberg (1995)
14. Patarin, J., Courtois, N., Goubin, L.: SFLASH, a Fast Multivariate Signature Algorithm (2003), `http://eprint.iacr.org/`
15. Shamir, A.: Efficient Signature Schemes Based on Birational Permutations. In: Stinson, D.R. (ed.) CRYPTO 1993. LNCS, vol. 773, pp. 1–12. Springer, Heidelberg (1994)
16. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. 26(5), 1484–1509 (1997)
17. Stein, W., et al.: Sage Mathematics Software (Version 4.6.2). The Sage Development Team (2011), `http://www.sagemath.org`
18. Wolf, C., Preneel, B.: Equivalent Keys in HFE, C*, and Variations. In: Dawson, E., Vaudenay, S. (eds.) Mycrypt 2005. LNCS, vol. 3715, pp. 33–49. Springer, Heidelberg (2005)

A Mathematical Results

Lemma 8. *Let* $\mathbf{P} = \lambda A + \mu B$ *be a matrix pencil over* $\mathbb{K}$*, symmetric and with null diagonal, of any dimension* n*. Its determinant is a bivariate form of degree* n*. If* n *is odd,* $\det(M) = 0$*, and if* n *is even, there exists a bivariate form* k *over* $\mathbb{K}$ *of degree* $n/2$ *such that* $\det(M) = k^2$*.*

Proof. We will prove this result using a recurrence in a 2 by 2 step. For $n = 1$, $M = (0)$ and $\det(M) = 0$. For $n = 2$, we have $M = \begin{pmatrix} 0 & k \\ k & 0 \end{pmatrix}$, where k is a bivariate form of degree 1 and $\det(M) = k^2$. Now, let $n \geq 3$ and assume the property is true for $n-2$. We will show that it is also true for n. We compute the determinant of M by developing according to the first column. Since the $(1,1)$-coefficient of M is null, we have $\det(M) = \sum_{i=2}^{n} M_{i,1} \det(M_{\overline{i}}^{\overline{1}})$, where $M_{i,1}$ denote the coefficient $(i,1)$ of M and $\det(M_{\overline{i}}^{\overline{1}})$ the $(1,i)$ minor. We can see that in all these minors, the first row has never been removed and always the first column. We can now do a development according to the first row and using the multi-linearity of the determinant, we get $\det(M) = \sum_{i=2}^{n} \sum_{j=2}^{n} M_{i,1} M_{1,j} \det(M_{\overline{1,i}}^{\overline{1,j}})$, where $M_{\overline{1,i}}^{\overline{1,j}}$ denote the matrix M by removing the rows 1 and i and the columns 1 and j. Since M is symmetric, we can add together the terms (i,j) and (j,i) for $i \neq j$ and these terms vanish. The determinant that we compute is equal to $\det(M) = \sum_{i=2}^{n} M_{i,1}^2 \det(M_{\overline{1,i}}^{\overline{1,i}})$. Now we can use the recurrence assumption and if n is odd, $\det(M) = 0$ and if n is even, $\det(M) = \sum_{i=2}^{n} M_{i,1}^2 k_i^2 = (\sum_{i=2}^{n} M_{i,1} k_i)^2$, where the forms k_i, for $i = 2, \ldots, n$ are of degree $(n-2)/2$. Consequently, the degree of the form $\sum_{i=2}^{n} M_{i,1} k_i$ is $n/2$. □

Lemma 9. *Let $\mathbf{P}_{\lambda,\mu}$ be an arbitrary pencil of quadratic forms. There exist a family of bivariate polynomials $\{\mathbf{p}_i\}_{0\leq i\leq d}$ in $\mathbb{K}[x,y]$ such that p_i is of degree i, and the characteristic polynomial of the polar form of $\mathbf{P}$ is:*

$$\chi\left(\psi\left(\mathbf{P}_{\lambda,\mu}\right)\right) = \sum_{i=0}^{d} {\mathbf{p}_i}^2 \cdot X^{n-2i}.$$

Proof. The result follows from lemma 8. The coefficient of X^{n-i} in $\chi\left(\psi\left(\mathbf{P}_{\lambda,\mu}\right)\right)$ is the sum of all M minors obtained by choosing $n-i$ diagonal terms and removing the $(n-i)$ corresponding rows and columns. The minors obtained are of dimension i. □

B Simultaneous Diagonalization of Two Quadratic Forms

Lemma 10. $\psi(\mathbf{P})(c_i, c_j) = 0 \qquad for \qquad 0 \leq i, j \leq d.$

Proof. Let (λ,μ) and (λ',μ') two pairs of variables in $\mathbb{K}^2$ such that $\lambda\mu' + \lambda'\mu \neq 0$. Because $\widetilde{p}_S(\lambda,\mu)$ and $\widetilde{p}_S(\lambda',\mu')$ are the kernels of $\lambda\psi\left(\mathcal{P}_1\right) + \mu\psi\left(\mathcal{P}_2\right)$ and $\lambda'\psi\left(\mathcal{P}_1\right) + \mu'\psi\left(\mathcal{P}_2\right)$ respectively, we find:

$$\begin{aligned}(\lambda\psi\left(\mathcal{P}_1\right) + \mu\psi\left(\mathcal{P}_2\right))(\widetilde{p}_S(\lambda,\mu), \widetilde{p}_S(\lambda',\mu')) = 0\\ (\lambda'\psi\left(\mathcal{P}_1\right) + \mu'\psi\left(\mathcal{P}_2\right))(\widetilde{p}_S(\lambda,\mu), \widetilde{p}_S(\lambda',\mu')) = 0\end{aligned}$$

By linear combination, we have

$$\begin{aligned}(\lambda\mu' + \lambda'\mu)\psi\left(\mathcal{P}_1\right)(\widetilde{p}_S(\lambda,\mu), \widetilde{p}_S(\lambda',\mu')) = 0\\ (\lambda\mu' + \lambda'\mu)\psi\left(\mathcal{P}_2\right)(\widetilde{p}_S(\lambda,\mu), \widetilde{p}_S(\lambda',\mu')) = 0\end{aligned}$$

and since $(\lambda\mu' + \lambda'\mu) \neq 0$,

$$\begin{aligned}\psi\left(\mathcal{P}_1\right)(\widetilde{p}_S(\lambda,\mu), \widetilde{p}_S(\lambda',\mu')) = 0\\ \psi\left(\mathcal{P}_2\right)(\widetilde{p}_S(\lambda,\mu), \widetilde{p}_S(\lambda',\mu')) = 0.\end{aligned}$$

Finally, thanks to the linearity of $\psi\left(\mathcal{P}_1\right)$ and $\psi\left(\mathcal{P}_2\right)$, we get:

$$\begin{aligned}\sum_{i=0}^{d}\sum_{j=0}^{d} \psi\left(\mathcal{P}_1\right)(c_i, c_j) \cdot \lambda^{d-i}\mu^i{\lambda'}^{d-j}{\mu'}^j = 0\\ \sum_{i=0}^{d}\sum_{j=0}^{d} \psi\left(\mathcal{P}_2\right)(c_i, c_j) \cdot \lambda^{d-i}\mu^i{\lambda'}^{d-j}{\mu'}^j = 0.\end{aligned}$$ □

Lemma 11. *For any family $\{r_i\}_{0\leq i\leq d}$ of polynomials over $\mathbb{K}$, we have:*

$$\mathbf{P}\left(\sum_{i=0}^{d} r_i \cdot c_i\right) = \sum_{i=0}^{d} {r_i}^2 \cdot \mathbf{P}(c_i).$$

Proof. We will prove it by induction on the number of non null polynomials in the family. We have $\mathbf{P}(r_1 \cdot c_1) = {r_1}^2 \cdot P(c_1)$ since $\mathbf{P}$ is a (pencil of) quadratic form(s) whose coefficients are bivariate polynomials over $\mathbb{K}$. Let us assume that the result holds for $k-1$ polynomials. According to the definition of the polar form, we can write:

$$\mathbf{P}\left(\sum_{j=1}^{k} r_j \cdot c_j\right) =$$

$$\mathbf{P}(r_1 c_1) + \mathbf{P}\left(\sum_{j=2}^{k} r_j \cdot c_j\right) + \psi(\mathbf{P})\left(r_1 \cdot c_1, \sum_{j=2}^{k} r_j \cdot c_j\right) =$$

$${r_1}^2 \cdot P(c_1) + \sum_{j=2}^{k} {r_j}^2 \cdot \mathbf{P}(c_j) + \sum_{j=2}^{k} r_1 \cdot c_j \cdot \psi(\mathbf{P})(c_1, c_j).$$

And lemma 10 allows to conclude.

C Showing Independence of the Coefficients of a Polynomial

We concentrate on a simpler polynomial of the form $\prod_{i=0}^{d-1}(x + t^{q^i})$.

Definition 1. *Let $d \geq 1$ a positive integer. We call elementary symmetric polynomials of order d, the $d+1$ polynomials with d variables $\sigma_{i,d}$, $0 \leq i \leq d$ defined implicitly by:*

$$\prod_{i=1}^{d}(X + X_i) = \sum_{i=0}^{d} \sigma_{i,d}(X_1, \ldots, X_d) X^{d-i}.$$

We also recall the following lemma useful to prove that a family of elements in $\mathbb{F}$ is independent [7].

Lemma 12. *Let $A = \{\alpha_i\}_{0 \leq i \leq d}$ a family of elements of $\mathbb{F}$. The elements in A are independent if and only if the determinant of the matrix $(\alpha_i^{q^j})_{0 \leq i,j \leq d}$ is non null.*

Let t an element of $\mathbb{F}$. In a first step we try to find an equivalent condition to the fact that the coefficients of the polynomial $\prod_{i=0}^{d-1}(x + t^{q^i})$ are independent. These coefficients can be expressed using the elementary symmetric polynomials. They are equal to $\{\sigma_{i,d}(t, t^q, \ldots, t^{q^{d-1}})\}_{0 \leq i \leq d}$.

We describe some notations. We denote by $s_{i,d}$ and Δ_d the mapping over $\mathbb{F}$ defined by:

$$s_{i,d}(x) = \sigma_{i,d}(x, x^q, \ldots, x^{q^{d-1}}),$$
$$\Delta_d(x) = \det((s_{i,d}(x)^{q^j})_{0 \leq i,j \leq d}).$$

Using the above lemma, and these notations, we can say that the coefficients of the polynomial $\prod_{i=d+1}^{n}(x+t^{q^{2i\theta}})$ are independent if and only if $\Delta_d(t) \neq 0$. In the following, we try to compute some simple expression for Δ_d.

Lemma 13. *For d and i integers such that $0 \leq i \leq d$, the Frobenius mapping commute with the mappings $s_{i,d}$, i.e. for every $x \in \mathbb{F}$, $s_{i,d}(x^q) = s_{i,d}(x)^q$.*

Proof. The mappings $s_{i,d}(x)$ are by construction sums of elementary functions $x \mapsto x^{q^{j_1}+\ldots+q^{j_i}}$, $0 \leq j_1 < \ldots < j_i \leq d-1$. The Frobenius mapping is linear and commute with each of these monomials. □

Lemma 14. *For d and i integers such that $1 \leq i \leq d$, we have:*

$$s_{i,d}(x) + s_{i,d}(x^q) = s_{i-1,d-1}(x^q)(x + x^{q^i}).$$

Proof. We have the following relations:

$$\begin{array}{l}\prod_{i=0}^{d-1}(X + x^{q^i}) + \prod_{i=0}^{d-1}(X + x^{q^{i+1}}) = \\ (x + x^{q^i})\prod_{i=1}^{d-1}(X + x^{q^i}) = (x + x^{q^d})\prod_{i=0}^{d-2}(X + x^{q^{i+1}})\end{array}$$

and

$$\begin{aligned}\prod_{i=0}^{d-1}(X + x^{q^i}) &= \sum_{i=0}^{d} s_{i,d}(x)X^{d-i} \\ \prod_{i=0}^{d-1}(X + x^{q^{i+1}}) &= \sum_{i=0}^{d} s_{i,d}(x^q)X^{d-i} \\ \prod_{i=0}^{d-2}(X + x^{q^i}) &= \sum_{i=0}^{d} s_{i,d-1}(x)X^{d-1-i}.\end{aligned}$$

We get the desired equality by considering the coefficient X^{d-i}. □

Lemma 15. *For $d \geq 1$, we have:*

$$\Delta_d(x) = \Delta_{d-1}(x^q)(x + x^{q^d})^{1+q+\ldots+q^{d-1}}.$$

Proof. The function Δ_d is a determinant of dimension $d+1$. We can note that the first line is composed of $d+1$ times the value 1 since for $0 \leq j \leq d$, $s_{0,d}^{q^j} = 1^{q^j} = 1$. We do not change the value of the determinant by adding each column to its right neighbor. After this operation, the first line is composed of one time the value 1 and d times the value 0. After this addition and using lemma 14, the term $(i+1, j+1)$ is:

$$\begin{aligned}s_{i+1,d}(x)^{q^j} + s_{i+1,d}(x)^{q^{j+1}} &= (s_{i,d}(x) + s_{i,d}(x^q))^{q^j} \\ &= s_{i,d+1}(x^q)^{q^j}(x + x^{q^d})^{q^j},\end{aligned}$$

which correspond to the term (i, j) of $\Delta_{d-1}(x^q)$ times $(x+x^{q^d})^{q^j}$. By developing the determinant using its first row, we recover $\Delta_{d-1}(x^q)$ times the factors of each column, that is $\prod_{j=0}^{d-1}(x + x^{q^d})^{q^j}$. □

Theorem 7. *For $d \geq 1$,*

$$\Delta_d(x) = \prod_{i=1}^{d} (x + x^{q^i})^{q^{d-i}+\ldots+q^{d-1}}.$$

Proof. By induction. Indeed, the formula is straightforward for $d = 1$ and

$$\Delta_1(x) = \det \begin{pmatrix} 1 & 1 \\ x & x^q \end{pmatrix} = x + x^q.$$

Assume that it is true for $d-1$, one gets:

$$\Delta_{d-1}(x^q) = \prod_{i=1}^{d-1} (x^q + x^{q^{i+1}})^{q^{d-1-i}+\ldots+q^{d-2}}$$

$$\Delta_{d-1}(x^q) = \prod_{i=1}^{d-1} (x + x^{q^i})^{q^{d-i}+\ldots+q^{d-1}}.$$

Using the formula of lemma 15, we get the result. □