The Generating Series of Support Minors MinRank Ideals

Daniel Smith-Tone[1,2]

[1] University of Louisville, Louisville KY, USA
[2] National Institute of Standards and Technology, Gaithersburg, Maryland, USA
daniel.smith@nist.gov

Abstract. The support minors method has become indispensable to cryptanalysts in attacking various post-quantum cryptosystems in the areas of multivariate cryptography and rank-based cryptography. The complexity analysis for support minors minrank calculations is a bit messy, with no closed form for the Hilbert series of the ideal generated by the support minors equations (or, more correctly, for the quotient of the polynomial ring by this ideal).
In this article, we provide a generating series whose coefficients are the Hilbert Series of related MinRank ideals. This simple series therefore reflects and relates the structure of all support minors ideals. Its simplicity also makes it practically useful in computing the complexity of support minors instances.

Keywords: Multivariate Cryptography · Rank-Based Cryptography · Hilbert Series · MinRank.

1 Introduction

The MinRank problem, first studied in [8] is a natural computational linear algebra problem that has become an essential tool in the cryptanalysis of many multivariate post-quantum cryptosystems, e.g. [16,14,4,6,15,11,10,3,1,2,5]. In the last quarter of a century, many algorithms were developed to solve this problem, specifically in the context of cryptanalysis, see most significantly [13,11,10,17,3]. While each suggested algorithm may be the best in some regime of parameters, it seems for MinRank instances arising from most multivariate and rank-based cryptosystems that the support minors technique of [3] is the most efficient.

The complexity of support minors MinRank is well-established in [3], where formulas for the number of linearly independent equations at each degree are derived under a semi-regularity assumption. From these formulas, we can recover the Hilbert series for the support minors ideal; however, this series does not have a simple closed form and is rather unwieldy.

In this article, we compute something slightly deeper than the formulas of [3]. We derive a generating series for the Hilbert series, see [12], of *every* support minors MinRank instance. Specifically we derive a generating series whose coefficients are the Hilbert series for related support minors ideals.

Not only is this bi-series a new interesting object— connecting the structure of several related ideals, it has practical utility, as well. The bi-series has a simple closed form, making it trivial to compute solving degrees for any support minors ideal.

This article is organized as follows. In the next section, we introduce the support minors method of MinRank calculation and review the complexity analysis of [3]. We then derive the new generating series in the subsequent section. The subsequent section provides simple code to compute the solving degree of support minors instances.

2 Support Minors

In [3], the support minors method for solving MinRank was introduced. The method is based on the rank decomposition of the low rank matrix in the span of the given matrices.

Let $\mathbf{M}_1, \ldots, \mathbf{M}_K$ be $m \times n$ matrices with entries in some field $\mathbb{F}$. If there exists a linear combination

$$\mathbf{\Sigma} = \sum_{i=0}^{K} \lambda_i \mathbf{M}_i$$

of rank r, then it has a rank decomposition $\mathbf{\Sigma} = \mathbf{SC}$, where $\mathbf{S} \in \mathbb{F}^{m\times r}$ is the column support of $\mathbf{\Sigma}$ and $\mathbf{C} \in \mathbb{F}^{r\times n}$ is the row support of $\mathbf{\Sigma}$.

Given a row π_i of $\mathbf{\Sigma}$, we may form the composite matrix

$$\begin{bmatrix} \pi_i \\ \mathbf{C} \end{bmatrix},$$

which has rank r due to the fact that π_i is in the row space of $\mathbf{C}$. It then follows that all of the maximal minors of this matrix are zero.

The key observation is that via cofactor expansion along the added row, we may express each minor in terms of a coordinate of π_i and the maximal minors of $\mathbf{C}$. Allowing the unknown coefficients λ_i to be represented by variables x_i and allowing the unknown values of the maximal minors of $\mathbf{C}$ to be represented by variables c_J, where J is a subset of the columns of $\mathbf{C}$ of size r, each of the maximal minors of the composite matrix produces a bilinear polynomial in the polynomial ring $\mathbb{F}[X, C]$. The collection of all such support minors polynomials forms the support minors ideal I.

Due to the great number of minor variables, it is usually optimal to resolve the ideal I by using an XL-style algorithm, see [9] in which higher degree terms at bi-degree $(b, 1)$ are generated. Thus, we may restrict to the case that a single minor variable occurs in every monomial, and consider the algebra graded by degree in the linear variables. In this way, we may construct a Hilbert series and can avoid the necessity of a bi-series to capture the solving degree with respect to the two variable types.

In [3], the authors derive the solving degree of the support minors ideal under a semi-regularity assumption on the bilinear system. The main tool for the case in which the size of the field is larger than the solving degree is [3, Proposition 6], which states:

Proposition 1 *For any symmetric b-tensor S of dimension m and rank $b \geq 2$ over $\mathbb{F}_q$ with $q > b$ and for any subset J of $\{1, \ldots, n\}$ of size $r + b$, the following equation holds:*

$$\sum_{j_1=1}^{m} \cdots \sum_{j_b=1}^{m} S_{j_1,\ldots,j_b} \begin{vmatrix} \pi_{j_1} \\ \vdots \\ \pi_{j_b} \\ \mathbf{C} \end{vmatrix}_{*,J} = 0.$$

This proposition is the key tool for deriving relations among the generators of I, relations among the relations, and so on. This process produces an alternating sum revealing the number of linearly independent equations at each bi-degree $(b, 1)$,

$$\#\text{ l.i. eqs} = \sum_{i=1}^{b} (-1)^{i+1} \binom{n}{r+i} \binom{m+i-1}{i} \binom{K+b-i-1}{b-i}. \tag{1}$$

Equation (1) is valid as long as $q > b$ and $b < r + 2$, as explained in [3, Section 5.4]. We then conclude that if this quantity is greater than or equal to the number of monomials at bi-degree $(b, 1)$, namely $\binom{n}{r}\binom{K+b-1}{b}$, that the homogeneous ideal I is resolved.

In [3], a formula for the number of linearly independent equations at bi-degree $(b, 1)$ is also provided in the case $q = 2$ and $b < r + 2$ as well. In this case the number of linearly independent equations at bi-degree $(b, 1)$ is given by the formula

$$\#\text{ l.i. eqs} = \sum_{j=1}^{b} \sum_{i=1}^{j} (-1)^{i+1} \binom{n}{r+i} \binom{m+i-1}{i} \binom{K}{j-i}. \tag{2}$$

In principle we can derive formulas for the number of linearly independent equations at bi-degree $(b, 1)$ for every value of q, however, some small cases can be a bit awkward to work with and the greatest practical need is for instances in which either $q = 2$ or q is rather large in comparison to any solving degree that is useful. Thus, as in [3], we restrict our attention to these two important cases.

3 A New Type of Generating Series

From the analysis in [3] it is easy to derive a Hilbert series for the support minors ideal I with respect to the linear variables. We work with both cases from the previous section.

3.1 The Case $q > b$ and $b < r + 2$

At every bi-degree $(b, 1)$, the dimension of $\mathbb{F}_q[X, C]/I$ is given by the difference between the number of monomials at that bi-degree and the number of linearly independent homogeneous polynomials in the ideal at that bi-degree. Therefore, the Hilbert series for the support minors ideal associated with a (K, n, m, r) MinRank instance for $q > b$ and $b < r + 2$ is

$$\mathcal{H}(t) = \sum_{b=0}^{\infty}\sum_{i=0}^{b}(-1)^i\binom{n}{r+i}\binom{m+i-1}{i}\binom{K+b-i-1}{b-i}t^b.$$

Unfortunately, there is no closed form expression for this series in terms of rational functions.

We now change perspective and consider the target rank r (or equivalently the target dimension $n - r$ of the right kernel) as a parameter in the system, with the parameters K, n and m fixed, and derive a generating series for these Hilbert series across varying values of r. As a note, this method is generic and can work for any collection of parametrized systems of equations, though there is no reason a priori that we may obtain a nice closed form.

We define our bi-series $\mathcal{G}(s, t)$ by the relation

$$[s^{n-r}]\mathcal{G}(s, t) = \mathcal{H}(t),$$

where $[x^{n-r}]\mathcal{G}(x)$ represents the coefficient of s^{n-r}, represented as a polynomial in the variable t. This definition is sensible, since $\mathcal{H}(t)$ is determined by the parameters K, m, n and r. The bi-series $\mathcal{G}(s, t)$ incorporates information about every generic support minors MinRank instance for K matrices of dimension $m \times n$.

Expanding the product $\mathcal{H}(t)s^{n-r}$, we recover an obvious product structure in the bi-series. Specifically we observe that

$$\begin{aligned}\mathcal{H}(t)s^{n-r} &= \sum_{b=0}^{\infty}\sum_{i=0}^{b}(-1)^i\binom{n}{r+i}\binom{m+i-1}{i}\binom{K+b-i-1}{b-i}t^b s^{n-r}\\ &= \left(\sum_{i=0}^{\infty}(-1)^i\binom{n}{r+i}\binom{m+i-1}{i}t^i s^{n-r}\right)\left(\sum_{i=0}^{\infty}\binom{K+i-1}{i}t^i\right)\\ &= \left(\sum_{i=0}^{\infty}(-1)^i\binom{n}{r+i}\binom{m+i-1}{i}t^i s^{n-r}\right)\frac{1}{(1-t)^K}.\end{aligned}$$

Here, the first factor is very suggestive of a term in a product of series. Indeed, if we replace $\binom{n}{r+i}$ with the equivalent $\binom{n}{n-r-i}$, we find that the sum of the bottom entries of the binomial coefficients is $n - r$, the same as the power of s in that factor. Thus, we can express this factor as the term including s^{n-r} in a product of two series as follows:

$$\begin{aligned}\mathcal{H}(t)s^{n-r} &= \left(\sum_{i=0}^{\infty}\binom{n}{n-r-i}s^{n-r-i}(-1)^i\binom{m+i-1}{i}t^is^i\right)\frac{1}{(1-t)^K}\\ &= \left([s^{n-r}]\left(\sum_{i=0}^{\infty}\binom{n}{i}s^i\right)\left(\sum_{i=0}^{\infty}(-1)^i\binom{m+i-1}{i}t^is^i\right)\frac{1}{(1-t)^K}\right)s^{n-r}\\ &= \left([s^{n-r}]\frac{(1+s)^n}{(1+st)^m(1-t)^K}\right)s^{n-r}.\end{aligned}$$

Dividing by s^{n-r} on both sides and recalling the definition of $\mathcal{G}(s,t)$ we recover

$$\mathcal{G}(s,t) = \frac{(1+s)^n}{(1+st)^m(1-t)^K}. \tag{3}$$

We point out explicitly that though the polynomial ring $\mathbb{F}_q[X,C]$ has two disparate variable types, the variable s in the bi-series $\mathcal{G}(s,t)$ is not representing powers of the minor variables c_J at the solving degree. The variable s is instead tied to the corank of the target matrix, that is, the dimension of the cokernel when the matrix acts by right multiplication. In this sense $\mathcal{G}(s,t)$ is a generating series for support minors Hilbert series indexed by the target corank.

More directly, one may merely use $\mathcal{G}(s,t)$ to determine the solving degree of a support minors (m,n,r,K) MinRank instance whenever $q > b$ and $b < r+2$. The solving degree is given by

$$d_s = \min_b \left\{b : [t^b s^{n-r}]G(t,s) \leq 0\right\}. \tag{4}$$

3.2 The Case $q = 2$ and $b < r + 2$

We may use a similar method to recover a generating series for support minors Hilbert series in the case of $q = 2$ and $b < r+2$. In this case, we may use the fact that there are

$$\sum_{j=1}^{b}\binom{n}{r}\binom{K}{j}$$

monomials of bi-degree up to $(b,1)$ involving a minor variable c_J and recall Equation (2) to obtain the Hilbert series for the support minors ideal associated with a (K,n,m,r) MinRank instance in the $q=2$ case:

$$\mathcal{H}(t) = \sum_{b=1}^{\infty}\sum_{j=1}^{b}\sum_{i=0}^{j}(-1)^{i+1}\binom{n}{r+i}\binom{m+i-1}{i}\binom{K}{j-i}t^b.$$

This Hilbert series can be rewritten as

$$\begin{aligned}\mathcal{H}(t) &= \sum_{j=1}^{\infty}\sum_{i=0}^{j}\binom{n}{r+i}\binom{m+i-1}{i}\binom{K}{j-i}\sum_{b=j}^{\infty}t^b \\ &= \sum_{j=1}^{\infty}\sum_{i=0}^{j}\binom{n}{r+i}\binom{m+i-1}{i}\binom{K}{j-i}\frac{t^j}{1-t} \\ &= \frac{1}{1-t}\sum_{j=1}^{\infty}\sum_{i=0}^{j}\binom{n}{r+i}\binom{m+i-1}{i}\binom{K}{j-i}t^j.\end{aligned}$$

We observe a similar kind of product structure as we previously encountered in the $q > b$ case. For variety, this time we factor the Hilbert series before deriving the new generating series. Notice that

$$\begin{aligned}\mathcal{H}(t) &= \frac{1}{1-t}\left[\left(\sum_{i=0}^{\infty}(-1)^i\binom{n}{r+i}\binom{m+i-1}{i}t^i\right)\left(\sum_{i=0}^{\infty}\binom{K}{i}t^i\right)-\binom{n}{r}\right] \\ &= \frac{1}{1-t}\left[(1+t)^K\left(\sum_{i=0}^{\infty}(-1)^i\binom{n}{r+i}\binom{m+i-1}{i}t^i\right)-\binom{n}{r}\right].\end{aligned}$$

Now we use the same strategy as before and define our generating series $\mathcal{G}(s,t)$ by the relation $[s^{n-r}]\mathcal{G}(s,t) = \mathcal{H}(t)$. The method remains the same; we expand the product $\mathcal{H}(t)s^{n-r}$.

Proceeding, we obtain

$$\mathcal{H}(t)s^{n-r} = \frac{(1+t)^K}{1-t}\left(\sum_{i=0}^{\infty}(-1)^i\binom{n}{r+i}\binom{m+i-1}{i}t^is^{n-r}\right)-\binom{n}{r}\frac{s^{n-r}}{1-t}.$$

At this point the summation in the formula is the exact same one we encountered in the analysis of the case $q > b$. Using the same substitution, we obtain

$$\begin{aligned}\mathcal{H}(t)s^{n-r} &= \left([s^{n-r}]\frac{(1+s)^n(1+t)^K}{(1+st)^m(1-t)}\right)s^{n-r}-\binom{n}{r}\frac{s^{n-r}}{1-t} \\ &= \left([s^{n-r}]\frac{(1+s)^n(1+t)^K}{(1+st)^m(1-t)}\right)s^{n-r}-\left([s^{n-r}]\frac{(1+s)^n}{1-t}\right)s^{n-r} \\ &= \left([s^{n-r}]\left[\frac{(1+s)^n(1+t)^K}{(1+st)^m(1-t)}-\frac{(1+s)^n}{1-t}\right]\right)s^{n-r}.\end{aligned}$$

As before, dividing by s^{n-r} and using the definition of $\mathcal{G}(s,t)$, we recover

$$\mathcal{G}(s,t) = \frac{(1+s)^n(1+t)^K}{(1+st)^m(1-t)}-\frac{(1+s)^n}{1-t}.$$

This generating series, as well, may be used to determine the solving degree of a support minors (m,n,r,K) MinRank instance whenever $q = 2$ and $b < r+2$. The solving degree is once again given by

$$d_s = \min_b\left\{b : [t^bs^{n-r}]G(t,s) \le 0\right\}. \qquad (5)$$

4 Computing the Solving Degree

For convenience, we provide simple code to compute the solving degree of support minors MinRank instances with the Magma Computer Algebra System[3], see [7]. The algorithms suppose input of the parameters for a MinRank instance including, K, the number of matrices, m, the number of rows, n, the number of columns, and r, the target rank.

Algorithm 1 SMSolvingDegree

```
Input: MinRank Parameters $(K, m, n, r)$
Output: Solving degree $b$.
$P\langle s\rangle$:=PowerSeriesRing(Integers());
$P\langle t\rangle$:=PowerSeriesRing($P$);
$f$:= $(1+s)^n/((1+st)^m(1-t)^K)$;
$b = 0$;
while Coefficient(Coefficient($f$,$b$),$n-r$) gt 0 do
    $b$+:= 1;
end while;
return $b$;
```

Algorithm 2 SMSolvingDegree2

```
Input: MinRank Parameters $(K, m, n, r)$
Output: Solving degree $b$.
$P\langle s\rangle$:=PowerSeriesRing(Integers());
$P\langle t\rangle$:=PowerSeriesRing($P$);
$f$:= $((1+s)^n(1+t)^K/((1+st)^m(1-t)) - (1+s)^n/(1-t)$;
$b = 0$;
while Coefficient(Coefficient($f$,$b$),$n-r$) gt 0 do
    $b$+:= 1;
end while;
return $b$;
```

The code for the case $q > b$ and $b < r+2$ is given in Algorithm 1, whereas the code for the case of $q = 2$ and $b < r+2$ is provided in Algorithm 2. Both of the provided algorithms should be placed in a function environment. There are multiple options for the syntax for such functions. An example of such

[3] Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement of any product or service by NIST, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose.

syntax would be **function SMSolvingDegree**(K, m, n, r) followed by the code provided and terminated with **end function;**.

As another disclaimer, this code provides the solving degree of a generic support minors system with the specified parameters. In actually computing the complexity of a support minors MinRank calculation other matters must be taken into consideration for optimizing the complexity. In general, one needs to optimize over possible choices for the number of columns, for example, to achieve best results.

5 Conclusion

This article provides a simple technique to construct a new type of generating series encoding the structure of ideals related by a parameter. In principle, this method can be used for any parametrized family of ideals, though there is no obvious reason that the resulting series should have a nice closed form.

In the case of support minors ideals, constructed to solve the important MinRank problem from computational linear algebra, however, the method produces a simple closed form for this "master series," even though the known Hilbert series for individual support minors ideals itself has no closed form. Instead, this new generating series uses a new variable and encodes the Hilbert series for the support minors ideals indexed by the corank of the target low rank matrix.

In addition to the interesting fact that we have a single generating series encoding the structure of all support minors instances of a certain size simultaneously, this series has a practical utility as well. The simple series makes it much easier to derive the solving bi-degree of support minors systems in code. We provide a few lines of working MAGMA code that computes the solving bi-degree $(b, 1)$ of such support minors systems.

References

1. Apon, D., Moody, D., Perlner, R.A., Smith-Tone, D., Verbel, J.A.: Combinatorial rank attacks against the rectangular simple matrix encryption scheme. In: Ding, J., Tillich, J. (eds.) Post-Quantum Cryptography - 11th International Conference, PQCrypto 2020, Paris, France, April 15-17, 2020, Proceedings. Lecture Notes in Computer Science, vol. 12100, pp. 307–322. Springer (2020). https://doi.org/10.1007/978-3-030-44223-1_17, https://doi.org/10.1007/978-3-030-44223-1_17
2. Baena, J., Briaud, P., Cabarcas, D., Perlner, R.A., Smith-Tone, D., Verbel, J.A.: Improving support-minors rank attacks: Applications to GeMSS and rainbow. In: Dodis, Y., Shrimpton, T. (eds.) Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part III. Lecture Notes in Computer Science, vol. 13509, pp. 376–405. Springer (2022). https://doi.org/10.1007/978-3-031-15982-4_13, https://doi.org/10.1007/978-3-031-15982-4_13
3. Bardet, M., Bros, M., Cabarcas, D., Gaborit, P., Perlner, R.A., Smith-Tone, D., Tillich, J., Verbel, J.A.: Improvements of algebraic attacks for solving the rank

decoding and minrank problems. In: Moriai, S., Wang, H. (eds.) 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. Lecture Notes in Computer Science, vol. 12491, pp. 507–536. Springer (2020). https://doi.org/10.1007/978-3-030-64837-4_17, https://doi.org/10.1007/978-3-030-64837-4_17

4. Bettale, L., Faugère, J., Perret, L.: Cryptanalysis of hfe, multi-hfe and variants for odd and even characteristic. Des. Codes Cryptogr. **69**(1), 1–52 (2013). https://doi.org/10.1007/s10623-012-9617-2, https://doi.org/10.1007/s10623-012-9617-2
5. Beullens, W.: Improved cryptanalysis of UOV and rainbow. In: Canteaut, A., Standaert, F. (eds.) Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part I. Lecture Notes in Computer Science, vol. 12696, pp. 348–373. Springer (2021). https://doi.org/10.1007/978-3-030-77870-5_13, https://doi.org/10.1007/978-3-030-77870-5_13
6. Beullens, W.: Breaking rainbow takes a weekend on a laptop. In: Dodis, Y., Shrimpton, T. (eds.) Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part II. Lecture Notes in Computer Science, vol. 13508, pp. 464–479. Springer (2022). https://doi.org/10.1007/978-3-031-15979-4_16, https://doi.org/10.1007/978-3-031-15979-4_16
7. Bosma, W., Cannon, J., Playoust, C.: The magma algebra system i: The user language. J. Symb. Comput. **24**(3–4), 235–265 (Oct 1997). https://doi.org/10.1006/jsco.1996.0125, https://doi.org/10.1006/jsco.1996.0125
8. Buss, J.F., Frandsen, G.S., Shallit, J.O.: The computational complexity of some problems of linear algebra. Journal of Computer and System Sciences **58**(3), 572–596 (1999). https://doi.org/https://doi.org/10.1006/jcss.1998.1608, https://www.sciencedirect.com/science/article/pii/S0022000098916087
9. Courtois, N.T., Klimov, A., Patarin, J., Shamir, A.: Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In: Preneel, B. (ed.) Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding. Lecture Notes in Computer Science, vol. 1807, pp. 392–407. Springer (2000). https://doi.org/10.1007/3-540-45539-6_27, https://doi.org/10.1007/3-540-45539-6_27
10. Faugère, J., Levy-dit-Vehel, F., Perret, L.: Cryptanalysis of minrank. In: Wagner, D.A. (ed.) Advances in Cryptology - CRYPTO 2008, 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008. Proceedings. Lecture Notes in Computer Science, vol. 5157, pp. 280–296. Springer (2008). https://doi.org/10.1007/978-3-540-85174-5_16, https://doi.org/10.1007/978-3-540-85174-5_16
11. Goubin, L., Courtois, N.T.: Cryptanalysis of the TTM cryptosystem. In: Okamoto, T. (ed.) Advances in Cryptology - ASIACRYPT 2000, 6th International Conference on the Theory and Application of Cryptology and Information Security, Kyoto, Japan, December 3-7, 2000, Proceedings. Lecture Notes in Computer Science, vol. 1976, pp. 44–57. Springer (2000). https://doi.org/10.1007/3-540-44448-3_4, https://doi.org/10.1007/3-540-44448-3_4

12. Hilbert: Ueber dietheorie der algebraischen formen. Mathematische Annalen **36**, 473–534 (1890), http://eudml.org/doc/157506
13. Kipnis, A., Shamir, A.: Cryptanalysis of the hfe public key cryptosystem by relinearization. Advances in Cryptology - CRYPTO 1999, Springer **1666**, 788 (1999)
14. Moody, D., Perlner, R.A., Smith-Tone, D.: An asymptotically optimal structural attack on the ABC multivariate encryption scheme. In: Mosca, M. (ed.) Post-Quantum Cryptography - 6th International Workshop, PQCrypto 2014, Waterloo, ON, Canada, October 1-3, 2014. Proceedings. Lecture Notes in Computer Science, vol. 8772, pp. 180–196. Springer (2014). https://doi.org/10.1007/978-3-319-11659-4_11, https://doi.org/10.1007/978-3-319-11659-4_11
15. Perlner, R.A., Petzoldt, A., Smith-Tone, D.: Total break of the SRP encryption scheme. In: Adams, C., Camenisch, J. (eds.) Selected Areas in Cryptography - SAC 2017 - 24th International Conference, Ottawa, ON, Canada, August 16-18, 2017, Revised Selected Papers. Lecture Notes in Computer Science, vol. 10719, pp. 355–373. Springer (2017). https://doi.org/10.1007/978-3-319-72565-9_18, https://doi.org/10.1007/978-3-319-72565-9_18
16. Tao, C., Petzoldt, A., Ding, J.: Efficient key recovery for all HFE signature variants. In: Malkin, T., Peikert, C. (eds.) Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part I. Lecture Notes in Computer Science, vol. 12825, pp. 70–93. Springer (2021). https://doi.org/10.1007/978-3-030-84242-0_4, https://doi.org/10.1007/978-3-030-84242-0_4
17. Verbel, J.A., Baena, J., Cabarcas, D., Perlner, R.A., Smith-Tone, D.: On the complexity of "superdetermined" minrank instances. In: Ding, J., Steinwandt, R. (eds.) Post-Quantum Cryptography - 10th International Conference, PQCrypto 2019, Chongqing, China, May 8-10, 2019 Revised Selected Papers. Lecture Notes in Computer Science, vol. 11505, pp. 167–186. Springer (2019). https://doi.org/10.1007/978-3-030-25510-7_10, https://doi.org/10.1007/978-3-030-25510-7_10