Polynomial Lattices for the BIKE Cryptosystem

Michael Schaller
E-mail: michael.schaller@math.uzh.ch

February 23, 2026

Abstract

In this paper we introduce a rank 2 lattice over a polynomial ring arising from the public key of the BIKE cryptosystem [1]. The secret key is a sparse vector in this lattice. We study properties of this lattice and generalize the recovery of weak keys from [3]. In particular, we show that they implicitly solved a shortest vector problem in the lattice we constructed. Rather than finding only a shortest vector, we obtain a reduced basis of the lattice which makes it possible to check for more weak keys.

1 Introduction and Related Work

One of the round 4 candidates of the NIST competition for Post-Quantum cryptography was the BIKE cryptosystem [1]. It has not been selected for standardization, but the related scheme HQC [11] will be standardized.

In this paper we construct a lattice over a polynomial ring to study the BIKE cryptosystem. The lattice is constructed from the public key while the secret key is a sparse vector in this lattice. We investigate the properties of this lattice, in particular the successive minima of the lattice.

Moreover, in our framework we can reinterpret the work from [3] in which a class of weak keys for BIKE has been exhibited. We extend their ideas using the work of Mahler [15] and Lenstra [14] on lattices over polynomial rings and reformulate the results of [3]. This enables us to give a more general perspective on the problem and to obtain more weak keys than in the original work in [3]. It turns out that (without using this perspective) they find a shortest vector in the lattice. Using the lattice we are able to obtain a reduced basis instead of just a shortest vector in the lattice which allows to test for more weak keys.

We would like to point out that the weak keys from [3] are not related to the weak keys that are studied in connection with decoding failure rates.

Our framework bears similarity to the function field decoding approach introduced in [7]. While they work on different problems, in particular a search to decision reduction, several of the general ideas about the BIKE cryptosystem and more generally quasi-cyclic codes are implicit in their work. Thinking about

the Minkowski embedding for rings of integers of number fields and classical lattices in the real numbers makes the connection to their work more obvious.

There have also been other works that investigated lattices over non-archimedean fields in other settings. Especially noteworthy are the works of Bernstein [6], Cohn and Heninger [9] who used an analogy with Coppersmith's theorem in order to reinterpret the Guruswami-Sudan list decoding algorithm. In addition, there have been applications to the computations of Riemann-Roch spaces, for example in Bauch's PhD thesis [4].

The structure of the paper is as follows. In Section 2 we briefly describe the BIKE cryptosystem and the weak key attack by the authors of [3]. In Section 3 we deal with lattices over $\mathbb{Z}$ and give some motivation for the use of polynomial lattices for BIKE later. In Section 4 we introduce and prove results needed later about lattices in the non-archimedean case. Section 5 contains the main part of the paper in which we introduce a lattice related to the BIKE cryptosystem and prove all the statements we need for the lattices in our treatment of the weak key attack on the BIKE cryptosystem. We conclude with Section 6.

2 The BIKE Cryptosystem and a Class of Weak Keys

First of all we describe the BIKE cryptosystem [1]. Let us fix a prime r such that 2 generates $\mathbb{F}_r^\times$. The secret key consists of two sparse (weight $v \sim \sqrt{r}$) elements $h_1, h_2 \in \mathbb{F}_2[x]/(x^r - 1)$. The public key is $\frac{h_1}{h_2}$. The goal of a key recovery attack is to recover h_1 and h_2 from h. Actually, we do not need the very same h_1 and h_2. Any two sparse elements h_1, h_2 satisfying $h = \frac{h_1}{h_2}$ are good enough.

Next we sketch the idea of the attack from [3]. Let us rewrite the equation for the public key as

$$h_1 = hh_2 \mod x^r - 1.$$

This gives us the rational reconstruction problem which can be solved uniquely by the extended Euclidean algorithm as long as $\deg(h_1) + \deg(h_2) < r$. The proof of uniqueness is in essence the same as the proof of Theorem 4.8 in [20]. The authors of [3] also use group actions that come from the code being quasi-cyclic and from the squaring map on $\mathbb{F}_2[x]/(x^r - 1)$ to get more weak keys. We will not describe it here, but only mention that one can do the same thing using the new approach from our paper.

More information about the rational reconstruction problem in the case of integers can be found in [20].

In the next sections we will give another perspective on the problem which we deem more natural and which allows to change the condition that $\deg(h_1) + \deg(h_2) < r$.

3 Lattices and Thue's Lemma

In this section we motivate the use of lattices in the later sections. The results here give an indication of what will happen in Sections 4 and 5 for polynomial lattices. Here we consider lattices as discrete subgroups of $\mathbb{R}^n$ (in contrast to the next sections where we consider lattices over polynomial rings). All the lattices are assumed to be full rank.

Let $\gamma \in \mathbb{Z}_{>0}$. Now we introduce γ-ary lattices (usually called q-ary lattices where γ is replaced by q). Let $k \leq n$ and $A \in \mathbb{Z}/(\gamma)^{k\times n}$ be a matrix. We define

$$\Lambda_\gamma^\perp(A) = \{x \in \mathbb{Z}^n : Ax = 0 \mod \gamma\}.$$

We get the following well known lemma.

Lemma 1. *Let $k \leq n$ and $A \in \mathbb{Z}/(\gamma)^{k\times n}$ be a matrix. Then*

$$\operatorname{covol}(\Lambda_\gamma^\perp(A)) \leq \gamma^k.$$

Proof. Let $\pi : \mathbb{Z}^n \to \mathbb{Z}/(\gamma)^n$ be the natural projection. Then

$$\Lambda_\gamma^\perp(A) = \pi^{-1}(\ker A).$$

Hence

$$\mathbb{Z}^n/\Lambda_\gamma^\perp(A) \cong (\mathbb{Z}/(\gamma)^n)/(\ker A) \cong \operatorname{im} A \subseteq \mathbb{Z}/(\gamma)^k.$$

The last inclusion implies the claim. □

We first state Thue's lemma which can be found for instance in [20] and then prove it using Minkowski's Theorem.

Lemma 2 (Thue)**.** *Let $\gamma, b, a^*, t^* \in \mathbb{Z}_{\geq 0}$. Assume $0 < a^* \leq \gamma < a^*t^*$. Then there exist $a, t \in \mathbb{Z}$ such that $|a| < a^*, 0 < |t| < t^*$ satisfying*

$$a \equiv bt \mod \gamma.$$

Proof. Consider the following lattice:

$$L = \{(a, t) : a - bt \equiv 0 \mod \gamma\}.$$

We want to estimate the covolume of the lattice in order to apply Minkowski's Theorem. We have the trivial inclusions $\gamma\mathbb{Z}^2 \subseteq L \subseteq \mathbb{Z}^2$. But more is true. $L = \{(a, t) \in \mathbb{Z}^2 : (1, -b)(a, t)^T \equiv 0 \mod \gamma\}$ is an γ-ary lattice. Thus, using Lemma 1, we get that

$$\operatorname{covol}(L) \leq \gamma.$$

Under the assumption that the volume of a convex, symmetric (around 0) body R is larger than 4γ, we get, using Minkowski's Theorem, a nonzero lattice point in R. The rectangle $R = \{(x_1, x_2) : |x_1| < a^*, |x_2| < t^*\}$ has volume $4a^*t^* > 4\gamma$. Hence there exists a nonzero lattice point in it. It is easy to see that if $t = 0$ we also get $a = 0$ and the statement is proven. □

Note that we could also additionally assume $a \geq 0$ since we will get a nonzero lattice point x and its inverse $-x$. In [20] the author gives an efficient algorithm relying on the extended Euclidean algorithm to give an explicit solution for Lemma 2. Note that this amounts to finding a short vector in a rank 2 lattice. So instead of the extended Euclidean algorithm we could run a lattice reduction algorithm like the Lagrange algorithm for rank 2 lattices.

4 Lattices over Polynomial Rings

In this section we explore the concept of a lattice over a polynomial ring $k[x]$ where k is a field. The study of this subject has been initiated by Mahler in [15] in which he treated an analogue of Minkowski's geometry of numbers [18] for non-archimedean fields. He also proved an analogue of Minkowski's Theorem. We will mainly be concerned with the paper by Lenstra [14] in which he presented a polynomial time algorithm for lattice reduction which ends up with a basis that has an orthogonality defect of 0. We will define lattices only over polynomial rings and not over general non-archimedean fields as done in [15]. For the purposes of this paper it is not even necessary to go to the field of rational functions or to Laurent series. We will also not go into the improvements of lattice reduction algorithms over polynomial rings like [19, 12] since for our purposes Lenstra's algorithm is sufficient.

We mainly recall the relevant results from [14], state the analogue of Minkowski's Theorem due to Mahler [15] and add a few results we could not find in the literature.

Definition 3. For $f \in \mathbb{F}_q[x]$ we define $|f| = \deg f$ for $f \neq 0$ and $|0| = -\infty$. We define the *norm* of $a = (a_1, \ldots, a_n) \in \mathbb{F}_q[x]^n$ as

$$|(a_1, \ldots, a_n)| = \max\{|a_1|, \ldots, |a_n|\}.$$

Note that $|f|$ for $f \in \mathbb{F}_q[x]$ does not behave like a non-archimedean norm, but like the additive inverse of a discrete valuation or equivalently like the logarithm of a non-archimedean norm.

Definition 4. Let $b_1, \ldots, b_n \in \mathbb{F}_q[x]^n$ be linearly independent over $\mathbb{F}_q[x]$. Then the *lattice* spanned by $b_1, \ldots, b_n$ is defined to be

$$L = \left\{ \sum_{i=1}^{n} \mu_i b_i : \mu_i \in \mathbb{F}_q[x] \right\}.$$

The *determinant* $\det(L)$ of the lattice is defined as the determinant of the matrix B which has $b_1, \ldots, b_n$ as rows. The *covolume* $\operatorname{covol}(L) = |\det(L)|$ of the lattice L is the degree of the determinant. The *orthogonality defect* of the basis $b_1, \ldots, b_n$ of the lattice L is defined to be

$$\operatorname{OD}(b_1, \ldots, b_n) = \left(\sum_{i=1}^{n} |b_i| \right) - |\det(L)|.$$

We call a basis with orthogonality defect 0 a *reduced* basis.

Remark 5. Note that $OD(b_1, \ldots, b_n) \geq 0$. Since the determinant of a lattice is unique up to elements in $\mathbb{F}_q^*$ we will consider the determinant only up to units. Moreover, since we work with the additive inverse of a valuation, we get after taking the orthogonality defect to an appropriate power (say $q^{\mathrm{OD}(b_1,\ldots,b_n)}$) the correct analogue of the usual definition of the orthogonality defect.

Next we define the analogue of an important classical notion for lattices.

Definition 6. The first *successive minimum* is defined to be the norm $|m_1|$ of a shortest non-zero vector m_1 in the lattice L. Iteratively we define the j-th successive minimum for $2 \leq j \leq n$ as follows. Take $j-1$ linearly independent vectors $m_1, \ldots, m_{j-1} \in L$ that attain the corresponding successive minima. The j-th *successive minimum* is the norm $|m_j|$ of a shortest vector $m_j \in L$ that is linearly independent of $m_1, \ldots, m_{j-1}$.

Remark 7. The value of the j-th successive minimum does not depend on the choice of the previous vectors $m_1, \ldots, m_{j-1}$.

Mahler defined a more general notion of successive minima with respect to more general convex bodies. Studying these could be an interesting problem for further research.

Lenstra proved the following result about the relation of successive minima and orthogonality defect.

Theorem 8 (Lenstra)**.** *Let $b_1, \ldots, b_n$ be a basis of the lattice L with $OD(b_1, \ldots, b_n) = 0$, ordered in such a way that $|b_1| \leq |b_2| \leq \ldots \leq |b_n|$. Then $|b_j|$ is the j-th successive minimum and in particular b_1 is a shortest vector of the lattice L.*

We will not describe the algorithm from Lenstra's paper, but we state the main result. Actually, the algorithm is not very long and also simple to implement.

Theorem 9 (Lenstra)**.** *Let $C > 0$ be such that $|b_i| \leq C$ for all $i \in \{1, \ldots, n\}$. Then there exists an algorithm that takes $O(n^3 C(\mathrm{OD}(b_1, \ldots, b_n)+1))$ arithmetic operations to transform a basis $b_1, \ldots, b_n$ of L into a reduced basis for L.*

In particular one can find a shortest vector in the given time. Note that one gets the following corollary using $\mathrm{OD}(b_1, \ldots, b_n) \leq nC$.

Corollary 10 (Lenstra)**.** *Let $C > 0$ be such that $|b_i| \leq C$ for all $i \in \{1, \ldots, n\}$. Then there exists an algorithm that takes $O(n^4 C^2)$ arithmetic operations to transform a basis $b_1, \ldots, b_n$ of L into a reduced basis for L.*

We will prove the following two lemmata since we could not find the statements and the proofs in the literature. However, they are not strictly necessary for the remainder of the paper. It is a classical result that for lattices $L_2 \subseteq L_1 \subseteq \mathbb{R}^n$ we have $[L_1 : L_2] = \frac{\mathrm{covol}(L_2)}{\mathrm{covol}(L_1)}$. We prove the following analogue.

Lemma 11. *Let $L_2 \subseteq L_1 \subseteq \mathbb{F}_q[x]^n$ be two lattices. Then*

$$[L_1 : L_2] = q^{\left|\frac{\det(L_2)}{\det(L_1)}\right|} = q^{\mathrm{covol}(L_2)-\mathrm{covol}(L_1)}.$$

Proof. By the elementary divisor theorem we can choose a basis $b_1, \ldots, b_n$ of L_1 and $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q[x]^*$ such that $\alpha_1 b_1, \ldots, \alpha_n b_n$ is a basis of L_2. Then by multilinearity of the determinant we get that

$$\det(L_2) = \left(\prod_{i=1}^{n} \alpha_i\right) \det(L_1).$$

Hence

$$\left|\frac{\det(L_2)}{\det(L_1)}\right| = \sum_{i=1}^{n} |\alpha_i|.$$

Furthermore,

$$[L_1 : L_2] = \prod_{i=1}^{n} q^{|\alpha_i|} = q^{\sum_{i=1}^{n} |\alpha_i|}.$$

This finishes the proof. □

We define an analogue of γ-ary matrices in this setting. Let $g \in \mathbb{F}_q[x]$. Further assume $k \leq n$ and $A \in \mathbb{F}_q[x]^{k\times n}$. We define

$$\Lambda_g^{\perp}(A) = \{a \in \mathbb{F}_q[x]^n : Aa \equiv 0 \mod g\}.$$

We have the following analogue to Lemma 1.

Lemma 12. *Let $k \leq n$ and $A \in \mathbb{F}_q[x]^{k\times n}$. Then*

$$[\mathbb{F}_q[x]^n : \Lambda_g^{\perp}(A)] \leq q^{|g|k}.$$

Proof. The proof is identical to the proof of Lemma 1. □

Using Lemma 11 we can also rewrite the previous lemma as $\mathrm{covol}(\Lambda_g^{\perp}(A)) \leq |g|k$.

Example 13. Let $A = (I_k|0_{n-k})$. Then

$$\Lambda_g^{\perp}(A) = (g\mathbb{F}_q[x]^k) \times \mathbb{F}_q[x]^{n-k}.$$

In this case, we get equality in Lemma 12. Namely,

$$\mathrm{covol}(\Lambda_g^{\perp}(A)) = |g|k.$$

Finally we will state the theorem by Mahler which is the analogue of Minkowski's Theorem in a slightly generalized form as in [2].

Theorem 14 (Mahler)**.** *Let L be a lattice and $|m_j|$ be its j-th successive minimum. Then*

$$\sum_{j=1}^{n} |m_j| = \mathrm{covol}(L).$$

Corollary 15 (Mahler)**.** *Let L be a lattice. Then for the first successive minimum $|m_1|$ we have $|m_1| \leq \frac{\text{covol}(L)}{n}$, i.e., there exists a non-zero lattice vector in L of norm at most $\frac{\text{covol}(L)}{n}$.*

5 BIKE from a Lattice Viewpoint

In the BIKE cryptosystem we have a similar problem as in Thue's Lemma 2 from Section 3, but in the polynomial setting. We want to solve

$$h_1 - hh_2 \equiv 0 \mod x^r - 1,$$

for h_1 and h_2 which are sparse. This problem has been studied as a problem of rational reconstruction (without the lattice viewpoint) in [3]. Again we can build a lattice

$$L = \{(h_1, h_2) : h_1 - hh_2 \equiv 0 \mod x^r - 1\}.$$

Note that this lattice can be constructed solely from the public key. We will propose a new algorithm to get weak keys in a similar way as in [3] by using lattice reduction and adding a possibility for using brute force. In practice our algorithm improves only very slightly upon the algorithm proposed before, but it gives a more unified perspective on it, especially since lattice reduction for polynomial rings over finite fields is computationally easy in general and not just for the 2-dimensional case as for the integers.

We can even write down an explicit basis for our lattice as we show in the following lemma.

Lemma 16. *Let $L = \{(h_1, h_2) : h_1 - hh_2 \equiv 0 \mod x^r - 1\}$. Then the vectors*

$$(x^r - 1, 0), (h, 1)$$

form a basis of L.

Proof. It is obvious that both vectors are in L. To show that they form a basis take $(h_1, h_2) \in L$. Then also

$$(h_1', 0) = (h_1, h_2) - h_2(h, 1) \in L.$$

But then

$$h_1' \equiv 0 \mod x^r - 1,$$

and consequently we can express (h_1, h_2) as a linear combination of $(x^r - 1, 0)$ and $(h, 1)$ with coefficients in $\mathbb{F}_q[x]$. □

Note that a similar result also holds for the case of the integers from Section 3. It is now easy to compute the determinant of L.

Corollary 17. *Let $L = \{(h_1, h_2) : h_1 - hh_2 \equiv 0 \mod x^r - 1\}$. Then the determinant of L is $x^r - 1$.*

Proof. The determinant of

$$\begin{pmatrix} x^r - 1 & 0 \\ h & 1 \end{pmatrix}$$

is $x^r - 1$. □

From Corollary 17 we get the following result for rational reconstruction, similar to Thue's Lemma 2.

Corollary 18. *Let* $L = \{(h_1, h_2) : h_1 - hh_2 \equiv 0 \mod x^r - 1\}$. *There exists* $a, b \in L$ *with* $|a| + |b| = r$. *In particular there exists* $a \in L$ *with* $|a| \leq \frac{r-1}{2}$.

Proof. We have $\text{covol}(L) = r$ from the previous corollary. By applying Theorem 14 we get the vectors a, b as desired. □

We could have also proven the statement using Lemma 12. In fact, for L as above we can compute a and b using Lenstra's algorithm. We get the following result from Lenstra's Corollary 10.

Lemma 19. *Let* $L = \{(h_1, h_2) : h_1 - hh_2 \equiv 0 \mod x^r - 1\}$. *Then one can find a reduced basis and hence also the successive minima of* L *in time* $O(r^2)$.

Now, let h_1 and h_2 be the actual private keys. In case that $|(h_1, h_2)| < \frac{r}{2}$, using Lemma 19, we recover essentially the attack from [3] since the attack from [3] usually computes the shortest vector a from Corollary 18. In [3] the authors also analyzed the probability that the condition on the degrees is satisfied.

We can now slightly extend this attack using brute force. It is worth mentioning that in the attack from [3] this is not possible since they only found a shortest vector, but no reduced basis. As long as the degrees of the private key are not too far from the degrees of the reduced basis we can compute the reduced basis and then try to find the private key as described in Algorithm 1.

Algorithm 1 Weak Keys via Lattice Reduction

Input:

- Public Key h for BIKE
- A bound B on the degree we use for brute force.

Step 1: Compute a reduced basis $a = (a_1, a_2), b = (b_1, b_2)$ for the lattice $L = \{(h_1, h_2) : h_1 - hh_2 \equiv 0 \mod x^r - 1\}$ using Lenstra's algorithm.
Step 2:
for $\mu_1, \mu_2 \in \mathbb{F}_2[x]_{<B}$ **do**
  Compute $(h_1', h_2') = \mu_1(a_1, a_2) + \mu_2(b_1, b_2)$.
  if h_1' and h_2' are sparse **then**
    return (h_1', h_2').
  end if
end for

However, there is a slight difference in the weak keys we get. In [3] they have the condition $\deg(h_1)+\deg(h_2) < r$, whereas we have the condition $|(h_1,h_2)| = \max\{\deg(h_1),\deg(h_2)\} < \frac{r}{2} + B$. Some of the weak keys from [3] we will not recover with Algorithm 1, and on the other hand some of our weak keys will not be recovered by the algorithm in [3]. Combining both approaches enables us to check for more (however not many more) weak keys than in the original paper. Using calculations similar to those in [3] we expect to gain at most a few bits upon the original attack for reasonable values on the bound B of the degree when using brute force. One can also apply to our approach the same improvements as in [3] using group actions which we have not considered here. In our case the analysis on the success probability follows along similar lines as in [3].

One problem on which the hardness of BIKE rests is the following.

Problem 20. *How hard is it to find short vectors in the lattice L where the norm is defined by $|(h_1,h_2)| = \mathrm{wt}(h_1) + \mathrm{wt}(h_2)$.*

However, while being a norm over $\mathbb{F}_q$ endowed with the trivial absolute value, this is not a norm over $\mathbb{F}_q(T)$ endowed with the absolute value arising from the degree and the natural norm on the lattice is quite far from the norm in Problem 20. Are there better algorithms to tackle this problem?

6 Conclusion and Open Questions

In this work we recast the rational reconstruction problem for key recovery of the BIKE cryptosystem as a problem of lattices over polynomial rings. Two questions that immediately arise are whether taking Mahler's [15] more general definition of successive minima can give more weak keys and whether they can be computed efficiently.

One of the main open questions is whether there are better key recovery attacks that use a similar approach. In particular, the lattice constructed in this paper is a rank 2 lattice and closely related to the Euclidean algorithm and continued fractions. Is there a way to construct a higher rank lattice that makes it possible to get (many) more keys?

We would like to point out that there have been two problems that started out with rank 2 lattices (or the extended Euclidean algorithm and continued fractions) and could be improved considerably using higher rank lattices. One is Wiener's classical attack [22] on small private keys using continued fractions and its improvements by Boneh and Durfee [8] relying on Coppersmith's attack [10] which uses the LLL algorithm. Another one is the decoding of Reed-Solomon codes by Berlekamp and Massey [5, 16] (reinterpreted as continued fractions by Mills [17], Welch and Scholtz [21]) and the breakthrough of List Decoding by Guruswami and Sudan [13] (reinterpreted by Bernstein [6], Cohn and Heninger [9] as an analogue of Coppersmith's theorem). Can something similar be done for the key recovery of the secret key of BIKE? At present this question is open and it requires new ideas.

In addition, it might also be worth applying similar methods to HQC [11].

Acknowledgements

I would like to thank Maxime Bombar for introducing me to the Function Field Approach for quasi-cyclic codes, which underlies cryptosystems like BIKE or HQC. Furthermore, I would like to thank him for mentioning the work of Bernstein, Cohn and Heninger on the Coppersmith Lattice Approach to List Decoding. In addition I would like to thank Paolo Santini for bringing [3] to my attention. I would also like to thank the reviewers for their valuable comments.

This work is supported by the Swiss National Science Foundation under SNSF grant number 212865.

References

[1] Nicolas Aragon, Paulo Barreto, Slim Bettaieb, Loic Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Philippe Gaborit, Santosh Ghosh, Shay Gueron, Tim Güneysu, Carlos Aguilar-Melchor, Rafael Misoczki, Edoardo Persichetti, Jan Richter-Brockmann, Nicolas Sendrier, Jean-Pierre Tillich, Valentin Vasseur, and Gilles Zémor. *BIKE: bit flipping key encapsulation*. 2024.

[2] Christian Bagshaw and Bryce Kerr. "Lattices in function fields and applications". In: *Mathematika* 71.2 (2025), e70010. DOI: 10.1112/mtk.70010.

[3] Magali Bardet, Vlad Dragoi, Jean-Gabriel Luque, and Ayoub Otmani. "Weak Keys for the Quasi-Cyclic MDPC Public Key Encryption Scheme". In: *Progress in Cryptology - AFRICACRYPT 2016 - 8th International Conference on Cryptology in Africa*. 2016. DOI: 10.1007/978-3-319-31517-1_18.

[4] Jens Dietrich Bauch. "Lattices over polynomial Rings and Applications to Function Fields". PhD thesis. Universitat Autònoma de Barcelona, 2014. URL: http://hdl.handle.net/10803/283357.

[5] Elwyn R Berlekamp. "Nonbinary BCH decoding". In: *University of North Carolina. Department of Statistics, Institute of Statistics Mimeo Series No. 502* (1966).

[6] Daniel J. Bernstein. "Reducing lattice bases to find small-height values of univariate polynomials". In: *Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography, Cambridge University Press* (2008). Ed. by J. P. Buhler and P.Editors Stevenhagen, pp. 421–446. DOI: 10.1017/9781139049801.014. URL: http://cr.yp.to/ntheory/smallheight-20051009.pdf.

[7] Maxime Bombar, Alain Couvreur, and Thomas Debris-Alazard. "On Codes and Learning with Errors over Function Fields". In: *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 (2022). Ed. by Yevgeniy Dodis and Thomas Shrimpton, pp. 513–540. DOI: 10.1007/978-3-031-15979-4_18.

[8] Dan Boneh and Glenn Durfee. "Cryptanalysis of RSA with private key d less than N/sup 0.292". In: *IEEE transactions on Information Theory* 46.4 (2000), pp. 1339–1349. DOI: 10.1109/18.850673.

[9] Henry Cohn and Nadia Heninger. "Ideal forms of Coppersmith's theorem and Guruswami-Sudan list decoding". In: *Adv. Math. Commun.* 9.3 (2015), pp. 311–339. DOI: doi.org/10.3934/amc.2015.9.311.

[10] Don Coppersmith. "Small solutions to polynomial equations, and low exponent RSA vulnerabilities". In: *Journal of cryptology* 10.4 (1997), pp. 233–260. DOI: 10.1007/s001459900030.

[11] Philippe Gaborit, Carlos Aguilar-Melchor, Nicolas Aragon, Slim Bettaieb, Loıc Bidoux, Olivier Blazy, Jean-Christophe Deneuville, Edoardo Persichetti, Gilles Zémor, Jurjen Bos, Arnaud Dion, Jérôme Lacan, Jean-Marc Robert, Pascal Véron, Paulo L. Barreto, Santosh Ghosh, Shay Gueron, Tim Güneysu, Rafael Misoczki, Jan Richter-Brockmann, Nicolas Sendrier, Jean-Pierre Tillich, and Valentin Vasseur. "Hamming Quasi-Cyclic (HQC)". In: (2025).

[12] Pascal Giorgi, Claude-Pierre Jeannerod, and Gilles Villard. "On the complexity of polynomial matrix computations". In: *Symbolic and Algebraic Computation, International Symposium ISSAC 2003, Drexel University, Philadelphia, Pennsylvania, USA, August 3-6, 2003, Proceedings* (2003). Ed. by J. Rafael Sendra, pp. 135–142. DOI: 10.1145/860854.860889.

[13] Venkatesan Guruswami and Madhu Sudan. "Improved decoding of Reed-Solomon and algebraic-geometric codes". In: *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280)*. 1998, pp. 28–37. DOI: 10.1109/sfcs.1998.743426.

[14] A.K. Lenstra. "Factoring multivariate polynomials over finite fields". In: *Journal of Computer and System Sciences* 30.2 (1985), pp. 235–248. ISSN: 0022-0000. DOI: 10.1016/0022-0000(85)90016-9.

[15] Kurt Mahler. "An analogue to Minkowski's geometry of numbers in a field of series". In: *Annals of Mathematics* 42.2 (1941), pp. 488–522. DOI: 10.2307/1968914.

[16] James Massey. "Shift-register synthesis and BCH decoding". In: *IEEE transactions on Information Theory* 15.1 (1969), pp. 122–127. DOI: 10.1109/tit.1969.1054260.

[17] William H Mills. "Continued fractions and linear recurrences". In: *Mathematics of Computation* 29.129 (1975), pp. 173–180. DOI: 10.2307/2005473.

[18] Hermann Minkowski. “Geometrie der Zahlen”. In: *BG Teubner* 1 (1910).

[19] Thom Mulders and Arne Storjohann. “On lattice reduction for polynomial matrices”. In: *J. Symb. Comput.* 35.4 (2003), pp. 377–401. DOI: 10.1016/S0747-7171(02)00139-6.

[20] Victor Shoup. “A Computational Introduction to Number Theory and Algebra”. In: *Cambridge University Press* (2008). DOI: 10.1017/cbo9780511814549. URL: https://shoup.net/ntb/.

[21] L Welch and R Scholtz. “Continued fractions and Berlekamp’s algorithm”. In: *IEEE Transactions on Information Theory* 25.1 (1979), pp. 19–27. DOI: 10.1109/tit.1979.1055987.

[22] Michael J Wiener. “Cryptanalysis of short RSA secret exponents”. In: *IEEE Transactions on Information theory* 36.3 (1990), pp. 553–558. DOI: 10.1109/18.54902.