Relinearization Attack on LPN over Large Fields

Paul Lou
pslou@cs.ucla.edu
UCLA

Amit Sahai
sahai@cs.ucla.edu
UCLA

Varun Sivashankar
varunsiva@ucla.edu
UCLA

Abstract

We investigate algebraic attacks on the Learning Parity with Noise (LPN) problem over large fields in parameter settings relevant to building indistinguishability obfuscation. In particular, we consider the setting where the proportion of equations that are corrupted with noise is inverse-polynomially sparse. Our hope was to obtain a subexponential algorithm using Macaulay expansion and relinearization. Alas, we did not find any such algorithm. Nevertheless, our findings propose an interesting relation between runtime and the rank of the Macaulay expansion.

If m is the number of initial equations, then the runtime of this attack is proportional to $O\left(2^{d \log m}\right)$ where d is the degree of Macaulay expansion. If the resulting system of equations has sufficiently large rank, we show that solving the LPN polynomial system requires a $O(\sqrt{m})$ degree expansion, which would imply a subexponential attack. Under the (more widely believed) assumption that the expanded system is semi-regular, however, we show that an $O(m)$ degree expansion is required to recover the secret vector.

In general, $O(\sqrt{m})$-degree expansions may not have sufficient rank for an attack. We propose a randomized algorithm to increase the rank of such expanded systems. Our algorithm introduces carefully chosen new equations to the system that hold with high probability to improve the likelihood of a successful attack. We highlight the empirical and theoretical challenges in analyzing this approach. The code for running the proposed algorithm is available at www.tinyurl.com/lpnattack.

1 Introduction

The LPN over large fields problem has been recently useful for a variety of cryptographic constructions [1, 2, 3, 4]. We study a relinearization attack, as used in the cryptanalysis on the binary Learning with Errors (LWE) problem[5, 6, 7], on the LPN problem over large fields. In particular, we use Macaulay expansion [6] in this context.

Let $n, m \geq 1$ be integers, q be an odd positive integer and $\mathbf{s} \in \mathbb{Z}_q^n$ be a secret vector. Suppose $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ is chosen uniformly at random, a noise vector $\mathbf{e} \in \mathbb{Z}_q^m$ is sampled according to a Bernoulli distribution, and we obtain $(\mathbf{A}, \mathbf{s}\cdot\mathbf{A}+\mathbf{e}) = (\mathbf{A}, \mathbf{b}) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^m$. The LPN search problem requires recovering $\mathbf{s} \in \mathbb{Z}_q^n$.

Define α_i for each $i \in [m]$ to be a variable that follows the following distribution:

$$\alpha_i = \begin{cases} 0 & \text{with probability } p = \frac{1}{n^\gamma} \\ 1 & \text{with probability } 1 - p = 1 - \frac{1}{n^\gamma} \end{cases} \tag{1}$$

For each $i \in [m]$, α_i can be interpreted as a Boolean indicator variable that takes the value of 1 if the error term e_i is 0 and takes the value of 0 if $e_i \neq 0$. Let $\alpha = (\alpha_1, \ldots, \alpha_m)$. Suppose we are given (or guess) the number of errors (zero terms) in α, say t. Then $t = m - \sum_{i=1}^m \alpha_i$. We thus have the following polynomial equation system $F = F_1 \cup F_2 \cup F_3$ where

$$F_1 = \left\{\alpha_i \langle \mathbf{a}^{(i)}, \mathbf{s}\rangle = \alpha_i b_i\right\}_{i=1}^m \qquad F_2 = \left\{\alpha_i^2 - \alpha_i = 0\right\}_{i=1}^m \qquad F_3 = \left\{t = m - \sum_{i=1}^m \alpha_i\right\}$$

2 Preliminaries

Notation For $n = n(\lambda)$, let $\mathsf{Ber}_\gamma(\mathbb{F})$ denote the Bernoulli distribution obtained by sampling a uniformly random element of $\mathbb{F}$ with probability $n^{-\gamma}$ and 0 with probability $1-n^{-\gamma}$ and let $\mathsf{Ber}_\gamma(\mathbb{F})^m$ denote the product distribution whose components are independently identically distributed from $\mathsf{Ber}_\gamma(\mathbb{F})$. We will use $x \xleftarrow{\$} \mathbb{F}$ to denote x sampling uniform randomly from $\mathbb{F}$. For two probabilities p, q, we denote $|p - q| \leq \epsilon$ by $p \approx_\epsilon q$.

Definition 2.1 (Learning Parity with Noise over Large Fields Assumption)**.** *For dimension $n = n(\lambda)$, number of samples $m = m(\lambda)$, and noise rate $\gamma(\lambda)$, the* $\mathsf{LPN}(n, m, \gamma)$ *problem is (T, ϵ)-hard if for any PPT adversary $\mathcal{A}$ that runs in time T, it holds that*

$$\begin{aligned} &\Pr\left[\mathbb{F} \leftarrow \mathcal{A}(1^\lambda), \mathbf{A} \xleftarrow{\$} \mathbb{F}^{m\times n}, \mathbf{e} \xleftarrow{\$} \mathsf{Ber}_\gamma(\mathbb{F})^m, \mathbf{s} \xleftarrow{\$} \mathbb{F}^n, \mathbf{b} \leftarrow \mathbf{A}\mathbf{s} + \mathbf{e} : \mathcal{A}(\mathbf{A}, \mathbf{b}) = 1\right] \\ &\quad \approx_\epsilon \Pr\left[\mathbb{F} \leftarrow \mathcal{A}(1^\lambda), \mathbf{A} \xleftarrow{\$} \mathbb{F}^{m\times n}, \mathbf{b} \leftarrow \mathbb{F}^m : \mathcal{A}(\mathbf{A}, \mathbf{b}) = 1\right] \end{aligned}$$

2.1 Linearization

Consider a polynomial system $F = \{f_i(\mathbf{x}) = 0\}_{i=1}^m$ where each $f_i(\mathbf{x}) \in \mathbb{Z}_q[x_1, \ldots, x_n]$. Then linearization refers to replacing every distinct monomial with a variable and treating the relabelled equations as a linear system in the new variables. In certain settings, we can perform linearization and solve the linear system. We can then use the values of the linearized variables to solve for the original values of $x_1, \ldots, x_n$.

2.2 Macaulay Expansion

The explanation of Macaulay expansion below has been taken almost verbatim from Sun et al. [6]. Consider the Arora-Ge approach of linearizing the polynomial system, except that we do not apply it to the quadratic system directly, but instead to an equivalent, expanded polynomial system. This expanded system is obtained by multiplying each equation of the form $f_i(\mathbf{x}) = 0$ by all possible monomials of degree up to d, for some fixed $d \geq 0$. The d-th Macaulay linear system is then the linear system obtained by taking this expanded polynomial system and linearizing it, i.e., replacing each monomial appearing in the system by a new variable. Since the maximum degree is $d + 2$, the resulting linear system consists of $m \cdot \binom{n+d}{d}$ equations in $\binom{n+d+2}{d+2}$ unknowns. The matrix of the system is called Macaulay matrix.

To give intuition for the Macaulay expansion, observe by Hilbert's Nullstellensatz that if there is unique solution (the secret vector) to our initial polynomial system, then the ideal generated by our initial polynomial system is equivalent to the ideal of polynomials that vanish on that secret vector:

$$\langle f_1, \ldots, f_m \rangle = \langle x_1 - s_1, \ldots, x_n - s_n \rangle.$$

Therefore, there exists some polynomials of minimal degree, $\{g_{i,j}\}_{i\in[m],j\in[n]}$ such that for $j \in [n]$,

$$x_j - s_j = g_{1,j} \cdot f_1 + \cdots + g_{m,j} \cdot f_m.$$

Consider the maximal degree monomial term in any $g_{i,j}$. The degree of this term is then the desired Macaulay expansion degree. Moreover, the ideal of polynomials for any Macaulay expanded system remains equivalent to that of the initial system (by definition of an ideal), so the solution to the d-th Macaulay expansion must assign s_j to the variable x_j.

2.3 Semi-Regularity

In the following imported definitions and imported lemma, we consider polynomials $f_1, \ldots, f_m \in \mathbb{F}[x_1, \ldots, x_n]$ for a field $\mathbb{F}$ for $m \geq n$.

Definition 2.2 (d-regular [8])**.** *A zero-dimensional overdetermined system $(f_1, \ldots, f_m)$ is d-regular when for all $i \in [m]$, if there exists polynomial g such that $\deg(g) < d - \deg(f_i)$ and $g \cdot f_i \in \langle f_1, \ldots, f_{i-1} \rangle$, then $g \in \langle f_1, \ldots, f_{i-1} \rangle$.*

Definition 2.3 (Degree of Semi-Regularity [8])**.** *The degree of semi-regularity of a zero dimensional ideal $\mathcal{I} \triangleq \langle f_1, \ldots, f_m \rangle$ is defined by*

$$d_{reg} = \min \left\{ d \geq 0 \mid \dim_{\mathbb{F}} \left(\{ f \in \mathcal{I}, \deg(f) = d \} = \binom{n+d-1}{d} \right) \right\}.$$

Definition 2.4 (Semi-regular systems [8])**.** *A d_{reg}-regular system is semi-regular.*

Lemma 2.5 (Imported from [8])**.** *For a semi-regular system with $m \geq n$ polynomials, the degree of semi-regularity is the index of the first non-positive coefficient in the series*

$$H(t) = \frac{\prod_{j=1}^{m}(1 - t^{\deg(f_j)})}{(1-t)^n}.$$

The complexity of a Macaulay attack has a computable upper bound, namely $O\left(\binom{n+d_{reg}}{d_{reg}}^{\omega}\right)$ where $\omega < 2.39$ is the linear algebra constant [6, 8]. Therefore, assuming a polynomial system is semi-regular, characterizing the attack complexity reduces to computing the degree of semi-regularity. In general, random quadratic polynomial systems are believed to be semi-regular, however no proof is known.

3 Potential Attack Strategies

3.1 Macaulay Expansion

Theorem 3.1. *Consider an* $\mathsf{LPN}(n, m, \gamma)$ *instance with* $m \geq n$. *Consider the Macaulay system obtained by expanding* $F = F_1 \cup F_2 \cup F_3$ *with degree of expansion* d. *Let the number of equations and number of linearized variables obtained from monomials in the expanded system be* E_d *and* V_d *respectively. Then if* $d = O(\sqrt{m})$, $V_d \leq E_d$.

Proof. Note that every equation in F_1 and F_2 has degree 2. When we multiply the above system by monomials to generate a Macaulay matrix, we need to multiply both F_1 and F_2 with monomials up to degree d.

Let $N = n + m$ be the number of variables in our system consisting of the n coordinates of the secret vector s and the m Boolean indicator variables $\{\alpha_i\}_{i \in [m]}$. With N variables, we have $\binom{N+d}{d}$ monomials of degree at most d by straightforward counting. Note that we have a total of $2m + 1$ initial equations from F_1, F_2, and F_3.

After Macaulay expansion with degree d, the number of equations E_d is given by $E_d = (2m + 1)\binom{N+d}{d}$. The number of monomials in the expanded system V_d is bounded by the number of degree monomials of degree at most $d+2$, that is, $V_d \leq \binom{N+d+2}{d+2}$. We want to find d large enough such that $V_d \leq E_d$. This happens when $\binom{N+d+2}{d+2} \leq (2m+1)\binom{N+d}{d}$. By simplifying the binomial coefficients, this is equivalent to $(N+d+2)(N+d+1) \leq (2m+1)(d+1)(d+2)$. Substituting $N = n+m$, we obtain a quadratic inequality in d: $(2m+1)(d+1)(d+2) - (d+n+m+2)(d+n+m+1) \geq 0$. The discriminant is given by

$$\Delta = 2m^3 + 4m^2 n + 2mn^2 + 2m^2 + 2mn + n^2 \leq 13m^3$$

We assume $m \geq n$. Solving for the larger root of the quadratic equation, $\frac{n-2m+\sqrt{\Delta}}{2m} \leq \frac{\sqrt{13m^3}}{2m} \leq 2\sqrt{m}$. □

This result brings up some interesting questions. Assuming the Macaulay expansion has sufficient rank, expanding with degree $d = O(\sqrt{m})$ suffices to solve for the secret vector s. This could potentially yield an attack running in time $O(2^{\sqrt{m}\log m})$, stronger than any previously known attack on LPN.

However, the rank of the system may not be high enough with only an $O(\sqrt{m})$ expansion because the number of variables grows along with the number of equations: for every new equation, we also introduce an equation in the indicator variable α_i. An alternate computation yields a less optimistic estimation of the degree of regularity. The computation below is very similar to Theorem 5 in [6].

Remark 3.2. For a discussion on semi-regularity and its relation to cryptographic settings, we refer the reader to [9], especially the discussion on the relevant conjectures noted on page 7.

Theorem 3.3. *Consider an* $\mathsf{LPN}(n, m, \gamma)$ *instance with* $m = n^{1+\alpha}$. *Consider the Macaulay system obtained by expanding* $F = F_1 \cup F_2 \cup F_3$ *with degree of expansion* d. *Let the number of equations and number of linearized variables obtained from monomials in the expanded system be* E_d *and* V_d *respectively. Then assuming semi-regularity, the degree of regularity of the system behaves asymptotically as*

$$d_{\text{reg}} \approx 0.09n^{1+\alpha} + 0.2n + 0.18n^{1-\alpha} + o(n^{-2\alpha}) = O(m)$$

Proof. In our LPN system of $2m+1$ equations, we can substitute $\alpha_1 = m - t - \sum_{i=2}^{m} \alpha_i$ into the first equation of F_1 and F_2, thus eliminating α_1 without changing the degree of any equation. So we have $E = 2m$ equations and $V = n + m - 1$ variables. Let h_d be the d^{th} coefficient of the Hilbert series below:

$$H_{E,V}(z) = \frac{(1-z^2)^E}{(1-z)^{V+1}} = \sum_{d=0}^{\infty} h_d z^d$$

The degree of regularity d_{reg} is the first value of d such that h_d is non-positive. In [6] (Theorem 5), it is shown that d must satisfy $d + 1 = E - \frac{V+1}{2} - \sqrt{E(E-V)}$. Then,

$$\begin{aligned}
d+1 &= 2m - \frac{n+m}{2} - \sqrt{2m(m-n+1)} \\
&= \frac{3}{2}m - \frac{n}{2} - \sqrt{2}m\sqrt{1 - \left(\frac{1}{n^\alpha} + \frac{1}{n^{1+\alpha}}\right)} \\
&= \left(\frac{3}{2} - \sqrt{2}\right)m + \left(\frac{1}{\sqrt{2}} - \frac{1}{2}\right)n + \frac{\sqrt{2}}{8}n^{1-\alpha} + o(n^{-2\alpha}) \\
&\approx 0.09n^{1+\alpha} + 0.2n + 0.18n^{1-\alpha} + o(n^{-2\alpha})
\end{aligned}$$

□

If d_{reg} is indeed $O(m)$, then Macaulay expansion is likely to be inefficient. However, we can potentially augment our initial system with additional equations that must hold with high probability. This could potentially boost the rank of the system even with a smaller degree of expansion.

3.2 Creating new equations with high degree

In an attempt to circumvent the pessimistic implications of Theorem 3.3 and boost the rank of the system without increasing the degree of expansion too much, we now introduce equations of high degree that hold with high probability. Note that the equation $\alpha_{i_1} \ldots \alpha_{i_d} = 0$ holds with high probability if the degree d is large enough because of the sparsity of LPN. The following theorem tells us how many such equations we can introduce that simultaneously hold with high probability. However, how to quantify the increase in rank with these additional equations is still unknown.

Theorem 3.4. *Consider an $\mathsf{LPN}(n, m, \gamma)$ instance with $m = n^{1+\alpha}$. We assume that the number of instances with errors is $t = \frac{m}{n^\gamma}$. Pick $\delta \in (0, 1)$ sufficiently small and $d \in \mathbb{Z}^+$ such that $d = \lceil n^{\gamma+\gamma'} \rceil$ where $\gamma' < 1 + \alpha$. Then we can introduce up to $k = \left\lfloor -\ln(1-\delta)2^{n^{\gamma'}} \right\rfloor$ equations of the form $\alpha_{i_1} \cdots \alpha_{i_d} = 0$ where the i_j are distinct for each equation, and all k equations hold with probability $1 - \delta$.*

Proof. The total number of degree d monomials multilinear in the α_i is $T = \binom{m}{d}$. The degree d monomials that will evaluate to 1 are the ones corresponding to a choice of d α_i's that are all chosen from the $m - t$ equations with no mistakes, so set $\Delta = \binom{m-t}{d}$. Therefore, the number of degree d monomials that will evaluate to 0 is given by $g = T - \Delta$. We want to ensure that the probability of k such random equations all hold is at least $1 - \delta$, so we require $\frac{g!}{(g-k)!}\frac{(T-k)!}{T!} \geq 1 - \delta$. Suppose $g \geq k - 1 > k - 1 - \Delta$. It follows that $p(g) \geq g^k$ and $q(g) \leq (g + \Delta)^k$. Then, $p(g) - (1-\delta)q(g) \geq g^k - (1-\delta)(g+\Delta)^k$. Rearranging terms, we have that the inequality is satisfied when $g \geq \frac{(1-\delta)^{\frac{1}{k}}}{1-(1-\delta)^{\frac{1}{k}}} \cdot \Delta$. Rearranging terms once again, this is equivalent to $k \leq \min\left(g + 1, -\frac{\ln(1-\delta)}{\ln(g+\Delta) - \ln(g)}\right)$. For δ small enough, it suffices for k to be smaller than the second term. So it suffices that $k \leq -\ln(1-\delta)\frac{g}{\Delta} =$

$-\ln(1-\delta)\left(\frac{\binom{m}{d}}{\binom{m-t}{d}}-1\right)$. Let the degree $d = \lceil n^{\gamma+\gamma'} \rceil$ for some parameter γ'. Recall that $t = \frac{m}{n^\gamma}$.

$$\left(\frac{\binom{m}{d}}{\binom{m-t}{d}}-1\right) \geq \left(\frac{m-d+1}{m-t-d+1}\right)^d \geq \left(\frac{m}{m-\frac{m}{n^\gamma}}\right)^d \geq 2^{\frac{d}{n^\gamma}} \geq 2^{n^{\gamma'}}$$

So we can introduce $\lfloor -\ln(1-\delta)2^{n^{\gamma'}} \rfloor$ equations of degree d that all hold with probability $1-\delta$. This analysis required that $d \leq m-t$, so assuming n is large enough, we can choose any γ' less than $1+\alpha$, although practically it may need to be a little smaller. □

Remark 3.5. To avoid confusion, let the degree of the equations we introduce with high probability be $r = \lceil n^{\gamma+\gamma'} \rceil$. Suppose we choose γ' such that $r = d_m$, where d_m is the degree of Macaulay expansion which guarantees $V_d \leq E_d$. Suppose we choose γ' appropriately such that $r = d$ (or perhaps $d+1$). Then in our Macaulay expanded system, we can eliminate a sub-exponential number of variables which could potentially significantly boost the rank of our expanded system.

Remark 3.6. We could fix γ', introduce some equations of degree $r = \lceil n^{\gamma+\gamma'} \rceil$ and then perform Macaulay expansion. We have not worked out the analysis, but it seems possible that introducing these new high degree equations to the $O(\sqrt{m}) = O(n^{\frac{1+\alpha}{2}})$ degree expansion would give sufficient rank for the linearization attack. Or alternately, it seems possible that an expansion degree of $O(m^{1-\eta})$ for $\eta > 0$ with the introduction of equations of degree $r' > r$ (pick larger γ') would provide sufficient rank for a linearization attack.

At this current in point in time, we do not know how these high degree equations exactly affect the rank.

4 Proof of Uniqueness

Note that in our set-up, we assume that we know what the number of mistakes t is. We run our algorithm for increasing values of t until we obtain a solution. However, we want to show that the solution we find is unique with high probability. Note that t follows a binomial distribution $B(m,p)$ where $p = \frac{1}{n^\gamma}$. Define $\mu = \frac{m}{n^\gamma}$. Let λ be a non-negative integer such that $\mu + \lambda \leq m$. Let $r = \mu + \lambda$.

Fact 4.1. *Suppose t follows a binomial distribution $B(m,q)$ with $r \geq \mu$ Then,* $\Pr(t \leq r) \geq 1 - \frac{r(1-p)}{(r-\mu)^2}$.

Theorem 4.2. *Consider an* $\mathsf{LPN}(n,m,\gamma)$ *instance with $m = n^{1+\alpha}$. Let the number of errors be t, and $\mu = \frac{m}{n^\gamma}$ the expected number of errors. Suppose $n^\gamma \geq 10$ Then with high probability $1 - \frac{4}{\mu}$, t is bounded by 2μ and there exists a unique secret vector $\mathbf{s} = (s_1, \ldots, s_n)$ satisfying the* LPN *instance.*

Proof. Let $r = \mu + \lambda$ for some integer λ. By Lemma 4.1 above, $\Pr(t \leq \mu + \lambda) \geq 1 - \frac{(\mu+\lambda)(1-p)}{\lambda^2} \geq 1 - \frac{\mu+\lambda}{\lambda^2}$. Suppose it is possible to solve the entire system for t_1 and t_2 to find s_1 and s_2 respectively where $t_1, t_2 \leq r = \mu+\lambda$ and $s_1 \neq s_2$. This means $\langle x_i, s_1 \rangle = \langle x_i, s_2 \rangle$ for at least $m - t_1 - t_2$ equations. So $\langle x_i, s_1 \rangle = \langle x_i, s_2 \rangle$ for at least $m' = m - 2r$ equations.

So for some matrix $\mathbf{A}' \in \mathbb{Z}_q^{m' \times n}$ with m' rows chosen from $\mathbf{A}$, $A'x = 0$ must have a non-zero solution. For this to not happen, every such matrix $\mathbf{A}'$ must have full rank n. We show that this happens with high probability. Consider any $m' = m - 2r \geq n$ rows chosen from the m rows of $\mathbf{A}$ to form $\mathbf{A}'$. Let $K = \binom{m}{m'} = \binom{m}{2r}$. We will choose q such that $q \geq m \geq n$. So $K \leq \frac{m^{2r}}{(2r)^{2r}} \leq \frac{q^{2r}}{(2r)^{2r}}$.

Call a vector $\mathbf{v} \in \mathbb{Z}_q^m$ *feasible* if it has at most $2r$ non-zero terms. It follows that

$$\Pr_{\mathbf{A}}(\exists \mathbf{x} \neq \mathbf{0} \in \mathbb{Z}_q^n : \mathbf{Ax} \text{ is feasible}) \leq \sum_{\mathbf{x} \in \mathbb{Z}_q^n - \{\mathbf{0}\}} \Pr_{\mathbf{A}}(\mathbf{Ax} \text{ is feasible}) = \sum_{\mathbf{x} \in \mathbb{Z}_q^n - \{\mathbf{0}\}} \frac{\binom{m}{2r} q^{2r}}{q^m} \leq \frac{q^{n+4r}}{(2r)^{2r} q^m}$$

$$\Pr\big(\text{rank}(\mathbf{A}') = n \; \forall \mathbf{A}'\big) \geq 1 - \frac{q^{n+4r}}{(2r)^{2r} q^m} = 1 - \frac{q^{n+4(\mu+\lambda)}}{(2r)^{2r} q^m}$$

Therefore, this LPN problem has a unique solution with probability at least $\left(1 - \frac{\mu+\lambda}{\lambda^2}\right)\left(1 - \frac{q^{4(\mu+\lambda)+n}}{q^m}\right)$. If we set $\lambda = \mu$ and assume $n^\gamma \geq 10$, the above probability is at least $1 - \frac{4}{\mu}$. □

5 Discussion

In this paper, we have suggested some directions to attack the LPN problem. Assuming sufficient rank, we have some bounds on the minimum degree required for Macaulay expansion, which is of the order $\mathcal{O}(n^{\frac{1+\alpha}{2}}) = O(\sqrt{m})$. However, the rank assumption is likely too strong, and an alternate computation suggests an estimate of $O(m)$ for the required degree of expansion to recover the secret vector. Introducing low degree equations that hold with high probability appears unlikely to change these asymptotics.

On the other hand, introducing equations with high degree using the indicator variables α_i to boost the rank of the Macaulay system might help us recover the secret vector. This definitely seems to be a promising direction, but with two main challenges:

1. Theoretical Challenge: Studying the rank of the vanilla Macaulay system is in itself quite difficult and it is not clear how to determine any bounds. Some trivial bounds can be obtained by counting the number of monomials, but this is unlikely to be of any use in proving that the expanded system has full rank (that is, the rank equals the number of monomials present). Further, determining whether introducing randomized equations produces a full rank matrix remains a challenge.

2. Empirical Challenge: While we have code available, the blow-up in the number of monomials makes it very difficult to test the behaviour of the algorithm for large values of n, m and d.

However, it is indeed possible that boosting the rank of the Macaulay matrix by setting certain high degree monomials to zero with high probability may be strong enough that a lower degree of expansion suffices. Further research in this direction could yield a different sub-exponential attack for the LPN problem.

5.1 Acknowledgements

We sincerely thank Aayush Jain for his insightful direction, especially on formulating our system of equations.

References

[1] Elette Boyle, Geoffroy Couteau, Niv Gilboa, and Yuval Ishai. Compressing vector ole. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, pages 896–912, 2018.

[2] Geoffroy Couteau and Pierre Meyer. Breaking the circuit size barrier for secure computation under quasi-polynomial lpn. In *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 II*. Springer-Verlag, 2021.

[3] Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, and Peter Scholl. Correlated pseudorandom functions from variable-density lpn. In *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1069–1080. IEEE, 2020.

[4] Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, and Peter Scholl. Efficient pseudorandom correlation generators from ring-lpn. In *Advances in Cryptology – CRYPTO 2020*. Springer International Publishing, 2020.

[5] Sanjeev Arora and Rong Ge. New algorithms for learning in presence of errors. In *International Colloquium on Automata, Languages, and Programming*, pages 403–415. Springer, 2011.

[6] Chao Sun, Mehdi Tibouchi, and Masayuki Abe. Revisiting the hardness of binary error lwe. In *Australasian Conference on Information Security and Privacy*, pages 425–444. Springer, 2020.

[7] Martin R. Albrecht, Carlos Cid, Jean-Charles Faugère, Robert Fitzpatrick, and Ludovic Perret. Algebraic algorithms for lwe problems. *ACM Commun. Comput. Algebra*, 49(2):62, aug 2015.

[8] Magali Bardet, Jean-Charles Faugère, and Bruno Salvy. On the complexity of grobner basis computation of semi-regular overdetermined algebraic equations. In *Proceedings of the International Conference on Polynomial System Solving (ICPSS 2004), November*, pages 71–75, 2004.

[9] M. Bigdeli, E. De Negri, M. M. Dizdarevic, E. Gorla, R. Minko, and S. Tsakou. Semi-regular sequences and other random systems of equations, 2020.