SCIS 2019 2019 Symposium on
Cryptography and Information Security
Shiga, Japan, Jan. 22 - 25, 2019
The Institute of Electronics,
Information and Communication Engineers

Sample-Time Trade-off for the Arora-Ge Attack on Binary-Error LWE

Sun Chao * Mehdi Tibouchi † Masayuki Abe ‡

Abstract: Binary-Error LWE is the particular case of the learning with errors problem in which errors are chosen uniformly in $\{0, 1\}$. It has various cryptographic applications, and in particular, has been used to construct efficient encryption schemes for use in constrained devices. Arora and Ge showed that the problem can be solved in polynomial time given a number of samples quadratic in the dimension n, but is known to be hard given only slightly more than n samples. It can also be solved in slightly subexponential time given a slightly superlinear number of samples, by applying Gröbner basis techniques to the system arising from Arora and Ge's approach. In this paper, we examine more generally how the hardness of the problem varies with the number of available samples, using a simpler (but asymptotically equivalent) variant of the Gröbner basis algorithm. In particular, under standard heuristics on the Arora-Ge polynomial system, we show that, for any $\varepsilon > 0$, Binary-Error LWE can be solved in polynomial time $n^{O(1/\varepsilon)}$ given $\varepsilon \cdot n^2$ samples. Similarly, it can be solved in subexponential time $2^{\tilde{O}(n^{1-\alpha})}$ given $n^{1+\alpha}$ samples, for $0 < \alpha < 1$. It is also easy to derive concrete complexity estimates for any given set of parameters, so as to evaluate the security of cryptographic schemes based on Binary-Error LWE.

Keywords: LWE, Binary-Error LWE, Cryptanalysis, Arora-Ge algorithm, Time complexity, Gröbner basis.

1 Introduction

The learning with errors problem (LWE), introduced by Regev in 2005 [11], is one of the central problems of lattice-based cryptography. It can be seen as an average-case problem which, for suitable parameters, is as hard as worst-case lattice problems, and it is therefore very convenient to build secure lattice-based cryptographic schemes: it has been used to build various primitives from encryption and signatures all the way to fully-homomorphic encryption.

For efficiency reasons, constructions often rely on variants of LWE (such as its ring version Ring-LWE [9]) or instantiations in more aggressive ranges of parameters than those for which Regev's reduction to worst-case lattice problems holds. An important example is *binary-error LWE*, where the error term is sampled uniformly from $\{0, 1\}$ (instead of from a wider discrete Gaussian distribution). Binary-Error LWE is a particularly simple problem with various interesting cryptographic applications, such as Buchmann et al.'s efficient lattice-based encryption scheme for IoT and lightweight devices [6] (based on the ring version of Binary-Error LWE, with the additional constraint that the secret is binary as well).

However, the problem is not hard given arbitrarily many samples: in fact, an algebraic attack due to Arora and Ge [3] solves Binary-Error LWE in polynomial time given around $n^2/2$ samples. The same approach can also be combined by Gröbner basis techniques to reduce the number of required samples [2]. On the other hand, Micciancio and Peikert [10] showed the Binary-Error LWE problem reduces to standard LWE (and thus is believed to be exponentially hard) when the number of samples is restricted to $n + O(n/\log n)$. Thus, the hardness of Binary-Error LWE crucially depends on the number of samples released to the adversary.

In this paper, we show that a simple extension of the Arora-Ge attack (based on similar ideas as the Gröbner basis approach, but simpler and at least as fast) provides a smooth time-sample trade-off for Binary-Error LWE: the attack can tackle any number of samples, with increasing complexity as the number of samples decreases. In particular, for Binary-Error LWE with $\varepsilon \cdot n^2$ samples ($\varepsilon > 0$ constant), we obtain an attack in polynomial time $n^{O(1/\varepsilon)}$, assuming standard heuristics on the polynomial system arising from the Arora-Ge approach. Similarly, for $n^{1+\alpha}$ samples ($\alpha \in (0, 1)$ constant), we obtain an attack in subexponential time $2^{\tilde{O}(n^{1-\alpha})}$. The precise complexity for any concrete number of samples is also easy to compute, which makes it possible to precisely set parameters for cryptographic schemes based on Binary-Error LWE.

* Kyoto University, Kyoto, Japan (sun.chao.46s@st.kyoto-u.ac.jp)
† NTT Secure Platform Laboratories , Tokyo, Japan
‡ NTT Secure Platform Laboratories , Tokyo, Japan

2 Preliminaries

2.1 Learning with Errors

The LWE problem asks to recover a secret $\mathbf{s} \in \mathbb{F}_q^n$, given a system of linear approximate equations. For instance,

$$\begin{aligned} 14s_1 + 15s_2 + 5s_3 + 2s_4 &\approx 8 \pmod{17} \\ 13s_1 + 14s_2 + 14s_3 + 6s_4 &\approx 16 \pmod{17} \\ 6s_1 + 10s_2 + 13s_3 + s_4 &\approx 3 \pmod{17} \\ 10s_1 + 4s_2 + 12s_3 + 16s_4 &\approx 12 \pmod{17} \\ 9s_1 + 5s_2 + 9s_3 + 6s_4 &\approx 9 \pmod{17} \\ 3s_1 + 6s_2 + 4s_3 + 5s_4 &\approx 16 \pmod{17} \end{aligned}$$

Each equation is satisfied up to some small error, sampled independently according to some known distribution (typically a discrete Gaussian distribution). The goal is to recover the secret $\mathbf{s}$. If the equation held without error, finding $\mathbf{s}$ would simply amount to solving a system of linear equations. We could therefore recover the secret $\mathbf{s}$ in polynomial time $O(n^\omega)$, where $2 \leq \omega \leq 3$ is the complexity exponent of linear algebra ($\omega \approx 2.37$ using the best known approach [8]). However, the errors introduced in LWE typically make the problem much harder. Formally, the LWE problem can be defined as follows.

Definition 2.1 (LWE)**.** The (search) LWE problem, defined with respect to a dimension n, a modulus q and an error distribution χ over $\mathbb{F}_q$, asks to recover a secret vector $\mathbf{s} \in \mathbb{F}_q^n$ given polynomially many samples of the form

$$\big(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e \bmod q\big) \in \mathbb{F}_q^n \times \mathbb{F}_q \tag{1}$$

where $\mathbf{a}$ is uniformly random in $\mathbb{F}_q^n$, and e is sampled according to χ. One can optionally specify the number $m = \mathrm{poly}(n)$ of available samples as an additional parameter.

Remark 2.1. One can also similarly define a decision variant of the LWE problem, which asks to distinguish the distribution of the samples (1) above from the uniform distribution over $\mathbb{F}_q^n \times \mathbb{F}_q$.

The LWE problem given m samples has a simple expression in matrix form: it asks to recover $\mathbf{s}$ from the pair $(A, \mathbf{b})$ where $A \in \mathbb{F}_q^{m \times n}$ is a uniformly random matrix, and $\mathbf{b} = A\mathbf{s} + \mathbf{e} \bmod q$, where all the coefficients of $\mathbf{e} \in \mathbb{F}_q^m$ are sampled independently from χ.

2.2 Cauchy Integral formula

Theorem 1 (Cauchy). Let C be a simple closed curve in the complex plane and f a holomorphic function on a region containing C and its interior. Assume C is oriented counterclockwise. Then for any z_0 inside C:

$$f(z_0) = \frac{1}{2\pi i} \oint_C \frac{f(z)}{z - z_0}\, dz.$$

Theorem 2 (Cauchy for derivatives). Under the same hypotheses, we have for all $n \geq 0$:

$$f^{(n)}(z_0) = \frac{n!}{2\pi i} \oint_C \frac{f(z)}{(z - z_0)^{n+1}}\, dz.$$

2.3 Laplace's method

Theorem 3. Let $\Phi\colon [a,b] \to \mathbb{R}$, $\psi\colon [a,b] \to \mathbb{C}$ be smooth functions. We assume that $\Phi'' > 0$ over $[a,b]$ and there exists $x_0 \in (a,b)$ such that $\Phi'(x_0) = 0$. Then, the following asymptotic estimate holds for $s \to +\infty$:

$$\int_a^b e^{-s\Phi(x)} \phi(x)\, dx = e^{-s\Phi(x_0)} \left[\frac{A}{\sqrt{s}} + O\Big(\frac{1}{s}\Big) \right]$$

where $A = \psi(x_0)\sqrt{2\pi/\Phi''(x_0)}$.

3 Binary-Error LWE

The Binary-Error LWE is simply the special case of Definition 2.1 where χ is the uniform distribution over $\{0,1\}$. In other words:

Definition 3.1 (Binary-Error LWE)**.** The Binary-Error LWE with parameters n, m and q asks to recover the vector $\mathbf{s} \in \mathbb{F}_q^n$ from m samples of the form:

$$\big(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e \bmod q\big) \in \mathbb{F}_q^n \times \mathbb{F}_q$$

where $\mathbf{a}$ is uniformly random in $\mathbb{F}_q^n$, and e is uniform in $\{0,1\}$.

The dimension n is the main security parameter, and both m and q are typically chosen as polynomially bounded functions of n. In this paper, we assume that $q = n^{\Theta(1)}$.

3.1 Uniqueness of solutions

Theorem 4. Suppose that the following condition is satisfied:

$$m \geq n \cdot \left(1 + \frac{c}{\log q}\right)$$

for some $c > \log 3$. Then, the Binary-Error LWE problem with parameters n, m, q has a unique solution with overwhelming probability.

Proof. Indeed, suppose that two solutions $\mathbf{s} \neq \mathbf{s}'$ exist to the Binary-Error LWE challenge $(A, \mathbf{b})$. This means that there exists binary error vectors $\mathbf{e}, \mathbf{e}'$ such that:

$$\mathbf{b} = A\mathbf{s} + \mathbf{e} = A\mathbf{s}' + \mathbf{e}'.$$

As a result, the vector $\mathbf{t} = \mathbf{s}' - \mathbf{s} \neq 0$ satisfies $A\mathbf{t} = \mathbf{e} - \mathbf{e}' \in \{-1, 0, 1\}^m$. It thus suffices to prove that for a random $A \in \mathbb{F}_q^{m \times n}$, such a vector $\mathbf{t}$ can only exist with negligible probability.

We can proceed as follows: fix $\mathbf{t} \in \mathbb{F}_q^n \setminus \{0\}$. For a uniformly random $A \in \mathbb{F}_q^{m \times n}$, the probability that $A\mathbf{t} \in \{-1, 0, 1\}^m$ is exactly $3^m/q^m$, since the product vector is uniformly distributed in $\mathbb{F}_q^m$. As a result, the union bound shows that:

$$\Pr_{A \xleftarrow{\$} \mathbb{F}_q^{m \times n}} \big[\exists \mathbf{t} \in \mathbb{F}_q^m \setminus \{0\}, A\mathbf{t} \in \{-1, 0, 1\}^m\big] \leq \left(\frac{3}{q}\right)^m \cdot q^n$$

since there are fewer than q^n possible vectors $\mathbf{t}$.

Therefore, assuming without loss of generality that $q > 3$, the probability ε that the challenge has at least two solutions is bounded as:

$$\begin{aligned}
\varepsilon &\leq \left(\frac{3}{q}\right)^m \cdot q^n \\
\log \varepsilon &\leq m \log\left(\frac{3}{q}\right) + n \log q \\
&\leq n\left(1 + \frac{c}{\log q}\right) \log\left(\frac{3}{q}\right) + n \log q \\
&= n\left(\log 3 - \log q + \frac{c \log 3}{\log q} - c + \log q\right) \\
&= n\big(\log 3 - c + o(1)\big)
\end{aligned}$$

and since $c > \log 3$, it follows that ε is negligible. □

3.2 Naive algorithm

From now on, we assume that the hypothesis of Theorem 4 is satisfied. It is easy to see that the matrix A is then of rank n with overwhelming probability (indeed, that probability is exactly $(1-q^{-m})(1-q^{1-m})\cdots(1-q^{n-1-m}) \geq 1 - q^{n-m}$, and this can be used to deduce a "naive" algorithm for Binary-Error LWE in time $O^*(2^n)$, essentially by guessing n coefficients of the error vector $\mathbf{e}$.

More precisely, since A is full rank, one can assume without loss of generality that its first n rows form an invertible square submatrix A_0. An algorithm for Binary-Error LWE is then as follows: guess the vector $\mathbf{e}_0 \in \{0,1\}^n$ consisting of the first n coefficients of $\mathbf{e}$; then deduce the corresponding $\mathbf{s} = A_0^{-1}(\mathbf{b}_0 - \mathbf{e}_0)$, and check that $\mathbf{e} = \mathbf{b} - A\mathbf{s}$ is indeed in $\{0,1\}^m$. The check is performed in $\mathrm{poly}(n)$ time, and by Theorem 4, there is with overwhelming probability a unique $\mathbf{e}_0 \in \{0,1\}^n$ passing this check, which corresponds to the unique solution $\mathbf{s}$. Trying all possibilities yields an algorithm in $O^*(2^n)$ time.

3.3 Arora–Ge algorithm

In a paper published at ICALP 2011, Arora and Ge proposed an algebraic approach to the LWE problem, which essentially amounts to expressing LWE as a system of *polynomial* equations, and then solving that system by unique linearization techniques. In the case of Binary-Error LWE, the polynomial system is a system of multivariate *quadratic* equations, which can be solved in polynomial time by linearization when the number m of samples exceeds about $n^2/2$.

More precisely, solving an instance $(A, \mathbf{b})$ of the Binary-Error LWE problem amounts to finding a vector $\mathbf{s} \in \mathbb{F}_q^n$ (which we have seen is uniquely determined) such that for $i = 1, \ldots, m$, we have:

$$b_i - \langle \mathbf{a}_i, \mathbf{s} \rangle \in \{0, 1\},$$

where the vectors $\mathbf{a}_i$ are the rows of A, and the scalars b_i the coefficients of $\mathbf{b}$. The idea of Arora and Ge is to rewrite that condition as:

$$\big(b_i - \langle \mathbf{a}_i, \mathbf{s} \rangle\big) \cdot \big(b_i - \langle \mathbf{a}_i, \mathbf{s} \rangle - 1\big) = 0,$$

which is a quadratic equation in the coefficients $s_1, \ldots, s_n$ of $\mathbf{s}$.

In general, solving a multivariate quadratic system is hard. However, it becomes easy when many equations are available. Arora and Ge propose to solve this system using a simple linearization technique: replace all the monomials appearing in the system by a new variable.

There are $\binom{n+2}{2} = (n+2)(n+1)/2$ monomials of degree at most 2. Therefore, if the number of samples m is at least $(n+2)(n+1)/2$, linearizing the quadratic system should yield a full rank linear system with high probability, and the secret $\mathbf{s}$ can be recovered by solving this linear system. This takes time $O\Big(\binom{n+2}{2}^\omega\Big) = O(n^{2\omega})$, and therefore shows that Binary-Error LWE can be solved in polynomial time given $m \approx n^2/2$ samples.

However, many applications of LWE-like problems only give out much fewer than $\Theta(n^2)$ samples. For example, public-key encryption schemes based on LWE-like problems often have a public key consisting of $O(n \log q)$ samples (or in some cases, just $O(n)$ samples). It is therefore interesting to analyze how the complexity of Binary-Error LWE varies as the number of available samples decreases. This is the goal of the present paper: more precisely, we describe an approach to extend the Arora–Ge attack to arbitrarily many samples at the cost of an increased attack complexity.

4 Our algebraic attack

4.1 Hilbert's Nullstellensatz for Arora–Ge

Slightly informally, Hilbert's Nullstellensatz essentially states that the ideal generated by a family of polynomials $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ coincides with the ideal of polynomials that vanish on the set $V(f_1, \ldots, f_m)$ of solutions of the polynomial system:

$$f_1(x_1, \ldots, x_n) = \cdots = f_m(x_1, \ldots, x_n) = 0.$$

Now consider the application of Hilbert's Nullstellensatz to the polynomial system arising from Arora and Ge's approach to Binary-Error LWE. That system is of the form:

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \qquad\qquad\vdots \\ f_m(x_1, \ldots, x_n) = 0 \end{cases} \tag{2}$$

where $f_1, \ldots, f_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ are known quadratic polynomials. By Theorem 4, the set $V(f_1, \ldots, f_m)$ of solutions of that system is reduced to a single point:

$$V(f_1, \ldots, f_m) = \big\{(s_1, \ldots, s_n)\big\} = \big\{\mathbf{s}\big\},$$

namely, the unique solution of the Binary-Error LWE problem. It follows[1] that the ideal $I = (f_1, \ldots, f_m) \subset$

[1] We are sweeping two technicalities under the rug. First, the set of solutions considered in the Nullstellensatz should really be computed over the algebraic closure of the base field; how-

$\mathbb{F}_q[x_1, \ldots, x_n]$ generated by the polynomials f_i coincides with the ideal of polynomial functions vanishing on $\{\mathbf{s}\}$, which is just $(x_1 - s_1, \ldots, x_n - s_n)$.

As a consequence, for $j = 1, \ldots, n$, there exist polynomials $g_1^{(j)}, \ldots, g_m^{(j)} \in \mathbb{F}_q[x_1, \ldots, x_n]$ such that:

$$g_1^{(j)} \cdot f_1 + \cdots + g_m^{(j)} \cdot f_m = x_j - s_j.$$

4.2 The Macaulay matrix

Now consider the Arora–Ge approach of linearizing the polynomial system, except that we do not apply it to the quadratic system (2) directly, but instead to an equivalent, *expanded* polynomial system. This expanded system is obtained from (2) by multiplying each equation $f_i = 0$ by all possible monomials of degree up to d, for some fixed $d \geq 0$. In other words, the equation $f_i = 0$ is replaced by the $\binom{n+d}{d}$ equations:

$$\begin{cases} f_i(s_1, \ldots, s_n) = 0 \\ s_1 f_i(s_1, \ldots, s_n) = 0 \\ \vdots \\ s_n f_i(s_1, \ldots, s_n) = 0 \\ s_1^2 f_i(s_1, \ldots, s_n) = 0 \\ s_1 s_2 f_i(s_1, \ldots, s_n) = 0 \\ \vdots \\ s_n^2 f_i(s_1, \ldots, s_n) = 0 \\ \vdots \\ s_n^d f_i(s_1, \ldots, s_n) = 0 \end{cases} \tag{3}$$

Of course, the resulting polynomial system, which consists of a total of $m\binom{n+d}{d}$ equations of degree $\leq d+2$ in n unknowns (since the f_i's are quadratic polynomials), is equivalent to the original system (2).

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 $m\binom{n+d}{d}$ equations in $\binom{n+d+2}{d+2}$ unknowns. The matrix of the system (for a certain ordering of the variables associated to the various monomials) is called the *Macaulay matrix*.

Consider then the polynomials $g_i^{(j)}$ introduced in the previous section (whose existence is guaranteed by the Nullstellensatz), and let d be the maximum of their total degrees. Clearly, the polynomial:

$$g_1^{(j)} \cdot f_1 + \cdots + g_m^{(j)} \cdot f_m$$

is a linear combination of the polynomials appearing in the expanded system (3) (since each term $g_i^{(j)} \cdot f_i$ can be seen as a linear combination of products of f_i by monomials of degree $\leq d$). But by definition, this polynomial is equal to $x_j - s_j$. Therefore, any solution of the d-th Macaulay linear system must assign the variable associated to x_j to s_j, the j-th coefficient of the actual solution $\mathbf{s}$.

This shows that for *some* sufficiently large d, one can solve Binary-Error LWE by solving the d-th Macaulay linear system. This is standard linear algebra on the Macaulay matrix of dimension $\binom{n+D}{D}$, where $D = d+2$ is the total degree of the polynomials in the expanded system, and therefore it can be carried out in time $O\left(\binom{n+D}{D}^\omega\right)$.

4.3 Semiregularity

One can completely determine the cost of the approach above provided that we can determine the minimal value D sufficient to recover $\mathbf{s}$, starting from a given number m of samples. This value D is called the *degree of regularity* of the system (2).

The degree of regularity is difficult to compute in complete generality, but has a tractable expression for a certain subclass of polynomial systems called *semiregular* polynomial systems. It is believed that random polynomial systems are semiregular with overwhelming probability, and therefore assuming semiregularity is a standard heuristic assumption.

We omit the formal definition of a semiregular system here. For our purposes, it suffices to give the explain how the degree of regularity of a semiregular system can be computed. Consider a polynomial system of m equations in n unknowns with $m > n$, defined by polynomials $f_1, \ldots, f_m$ of total degree $d_1, \ldots, d_m$ respectively, and introduce:

$$H(z) = \frac{\prod_{i=1}^m (1 - z^{d_i})}{(1 - z)^{n+1}}.$$

Note that this function H is a polynomial $1 + H_1 z + H_2 z^2 + \cdots$ with integer coefficients since $1 - z$ divides $1 - z^{d_i}$ for all i, and $m \geq n + 1$. If the polynomial system is semiregular, then its degree of regularity D is the smallest j such that the coefficient H_j of degree j of H satisfies $H_j \leq 0$.

4.4 Application to Binary-Error LWE

The Arora–Ge polynomial system arising from Binary-Error LWE is a polynomial system as above with $d_1 = \cdots = d_m = 2$. Therefore, we can sum up the results of this section as the following theorem.

Theorem 5. Under the standard heuristic assumption that the Arora–Ge polynomial system is semiregular, one can solve Binary-Error LWE in time $O\left(\binom{n+D}{D}^\omega\right)$, where D is the smallest j such that the coefficient of degree j of the following polynomial:

$$H(z) = \frac{(1 - z^2)^m}{(1 - z)^{n+1}} \tag{4}$$

is nonpositive.

ever, it is easy to see that the argument of Theorem 4 applies similarly to show uniqueness even for solutions on extensions of $\mathbb{F}_q$. Second, the Nullstellensatz actually describes the *radical* of the ideal $(f_1, \ldots, f_m)$, but it is clear that this ideal is already radical with overwhelming probability.

One can apply this result for concrete instances of the Binary-LWE problems. For example, the first two parameter sets proposed for the scheme of Buchmann et al. [6] correspond to the case when $n = 256$ and $m = 2n = 512$. One can easily check that the first nonpositive coefficient of $(1 - z^2)^{512}/(1 - z)^{257}$ is the coefficient of degree 30. Therefore, our algebraic attack reduces to solving a polynomial system in $\binom{256+30}{30} \approx 2^{135}$ unknowns.

The attack can in fact be improved due to the fact that the secret in that scheme is also binary, which provides n more quadratic equations of the form $s_i(s_i - 1) = 0$, for a total of 768. The first nonpositive coefficient of $(1-z^2)^{768}/(1-z)^{257}$ is the coefficient of degree 20, reducing the number of unknowns to $\binom{256+20}{20} \approx 2^{100}$. The resulting attack is better than the naive attack by guessing the error vector, but is worse than what can be achieved by lattice reduction techniques against the same parameters.

To estimate the complexity of the attack in more general cases, we simply need to find asymptotic estimates for the degree of the first nonpositive coefficient of the polynomial H from (4). This is the goal of the next section.

Remark 4.1 (Comparison to Gröbner bases). One can ask how this approach compares to simply applying Gröbner basis computation algorithm to the Arora–Ge polynomial system. The answer is that the two approaches are essentially equivalent (and in fact, some Gröbner basis algorithms such as Matrix-F4 for a suitable monomial ordering can be expressed in terms of Macaulay matrix [7]), but knowing the degree D in advance avoids the difficulties related to the iterative nature of Gröbner basis algorithms, and hence saves some polynomial factors in terms of asymptotic complexity. It also makes it clear that the problem reduces to solving a relatively sparse linear system (since the rows of the Macaulay matrix have only $O(n^2)$ nonzero coefficients among $O(n^D)$), which can yield to various algorithmic optimization.

Nevertheless, our results can be regarded as closely related to the Gröbner-based analysis presented in [1]. The main difference is that we are interested in a wider range of asymptotic regimes in order to obtain a full, smooth time-sample trade-off.

5 Sample-time trade-offs

As discussed above, estimating the asymptotic complexity of our algebraic attack reduces to computing the degree of regularity D of the Arora–Ge polynomial system, which, assuming semiregularity, is in turn equivalent to finding the degre of the smallest nonpositive coefficient of $H(z) = \frac{(1-z^2)^m}{(1-z)^{n+1}}$. This can be done using techniques from complex analysis, as demonstrated by Bardet et al. [4].

We apply those techniques in the following two asymptotic regimes: $m = \varepsilon \cdot n^2$ for some $\varepsilon > 0$, and $m = n^{1+\alpha}$ for some $\alpha \in (0, 1)$. The attack becomes polynomial time in the former case, and subexponential in the latter case.

Theorem 6. For $m = \varepsilon \cdot n^2$ (ε positive constant) quadratic equations in n variables, the degree of regularity D satisfies:

$$\lim_{n \to +\infty} D = \frac{1}{8\varepsilon} \tag{5}$$

The time complexity for Binary-Error LWE is thus $O\left(\binom{n+D}{D}^{\omega}\right) = n^{\omega/8\varepsilon + o(1)} = n^{O(1/\varepsilon)}$, which is polynomial time.

Theorem 7. For $m = n^{1+\alpha}$ (α is constant between 0 and 1) quadratic equations in n variables, the degree of regularity D satisfies

$$D \sim \frac{1}{8} n^{1-\alpha} \tag{6}$$

The time complexity for Binary-Error LWE is thus $O\left(\binom{n+D}{D}^{\omega}\right) = 2^{\tilde{O}(n^{1-\alpha})}$, which is subexponential time.

The two results are established similarly, so we only describe the proof of the first one.

5.1 Proof of Theorem 6

Proof. Denote h_d as the d-th coefficient of Hilbert series.

$$\mathrm{H}_{m,n}(z) = \frac{\left(1 - z^2\right)^m}{(1 - z)^n} = \sum_{d=0}^{\infty} h_d z^d \tag{7}$$

where the integration path enclose the origin and there are no other singularity of $H_{m,n}(z)$. Take d-th derivative for equation (1) and using Cauchy Integral formula for derivatives, we can get

$$\mathcal{I}_n(d) = \frac{1}{2i\pi} \oint H_{m,n}(z) \frac{dz}{z^{d+1}} = \frac{1}{2i\pi} \oint e^{nf(z)} dz \tag{8}$$

Then determine $f(z)$

$$\mathcal{I}_n(d) = e^{nf(z)} dz = \frac{1}{2i\pi} \oint g(z) e^{nf(z)} dz \tag{9}$$

Then we get

$$e^{nf(z)} = \frac{(1-z)^{m+n}(1+z)^m}{z^{d+1}} \tag{10}$$

Then we get $f(z)$

$$nf(z) = (m-n)\log(1-z) + m\log(1+z) - (d+1)\log z \tag{11}$$

Compute $f'(z)$

$$nf'(z) = \frac{n-m}{1-z} + \frac{m}{1+z} - \frac{d+1}{z} \tag{12}$$

Let $f'(z) = 0$

$$(n - 2m + d + 1)z^2 + nz - (d + 1) = 0 \tag{13}$$

If Δ of this equation is not zero, it means that there are two distinct saddle points. The contribution of

these two saddle points to the integral are conjugate values whose sum does not vanish. Hence the two saddle points must be identical, which means that $\Delta = 0$

$$\Delta = 4(d+1)^2 + 4(n-2m)(d+1) + n^2 = 0 \quad (14)$$

Solving this equation, we get

$$d + 1 = m - \frac{n}{2} - \sqrt{m(m-n)} \quad (15)$$

Substitute $m = \varepsilon n^2$

$$d + 1 = \varepsilon n^2 - \frac{n}{2} - \varepsilon n^2 \sqrt{1 - \frac{1}{\varepsilon n}} \quad (16)$$

Using taylor expansion

$$d + 1 \sim \frac{1}{8\varepsilon} \quad (17)$$

□

6 Conclusion

Assuming semiregularity, we get a concrete time analysis for Binary-Error LWE. The trade-off between time and samples can help us understand the hardness of Binary-Error LWE better. Hence, when building cryptographic schemes, we should consider the relation between time complexity and sample complexity before choosing security parameters.

References

[1] Martin Albrecht, Carlos Cid, Jean-Charles Faugere, Robert Fitzpatrick, and Ludovic Perret. Algebraic algorithms for lwe problems. 2014.

[2] Martin R Albrecht, Rachel Player, and Sam Scott. On the concrete hardness of learning with errors. *Journal of Mathematical Cryptology*, 9(3):169–203, 2015.

[3] 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.

[4] Magali Bardet, Jean-Charles Faugere, Bruno Salvy, and Bo-Yin Yang. Asymptotic behaviour of the index of regularity of quadratic semi-regular polynomial systems. In *The Effective Methods in Algebraic Geometry Conference (MEGA'05)(P. Gianni, ed.)*, pages 1–14. Citeseer, 2005.

[5] Bruno Buchberger, George E Collins, Rüdiger Loos, and Rudolph Albrecht. Computer algebra symbolic and algebraic computation. *ACM SIGSAM Bulletin*, 16(4):5–5, 1982.

[6] Johannes Buchmann, Florian Göpfert, Tim Güneysu, Tobias Oder, and Thomas Pöppelmann. High-performance and lightweight lattice-based public-key encryption. In *Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security*, pages 2–9. ACM, 2016.

[7] Jean-Charles Faugere. A new efficient algorithm for computing gröbner bases (f4). *Journal of pure and applied algebra*, 139(1-3):61–88, 1999.

[8] François Le Gall. Powers of tensors and fast matrix multiplication. In *Proceedings of the 39th international symposium on symbolic and algebraic computation*, pages 296–303. ACM, 2014.

[9] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 1–23. Springer, 2010.

[10] Daniele Micciancio and Chris Peikert. Hardness of sis and lwe with small parameters. In *Advances in Cryptology–CRYPTO 2013*, pages 21–39. Springer, 2013.

[11] Oded Regev. The learning with errors problem. *Invited survey in CCC*, 7, 2010.