The Influence of LWE/RLWE Parameters on the Stochastic Dependence of Decryption Failures

Georg Maringer[1]*, Tim Fritzmann[1]*, and Johanna Sepúlveda[2]

[1] Technical University of Munich, Munich, Germany
{georg.maringer,tim.fritzmann}@tum.de
[2] Airbus Defence and Space GmbH, Taufkirchen, Germany
johanna.sepulveda@airbus.com

Abstract. Learning with Errors (LWE) and Ring-LWE (RLWE) problems allow the construction of efficient key exchange and public-key encryption schemes. However, while improving the security through the use of error distributions with large standard deviations, the decryption failure rate increases as well. Currently, the independence of individual coefficient failures is assumed to estimate the overall decryption failure rate of many LWE/RLWE schemes. However, previous work has shown that this assumption is not correct. This assumption leads to wrong estimates of the decryption failure probability and consequently of the security level of the LWE/RLWE cryptosystem. An exploration of the influence of the LWE/RLWE parameters on the stochastic dependence among the coefficients is still missing. In this paper, we propose a method to analyze the stochastic dependence between decryption failures in LWE/RLWE cryptosystems. We present two main contributions. First, we use statistical methods to analyze the influence of fixing the norm of the error distribution on the stochastic dependence among decryption failures. The results have shown that fixing the norm of the error distribution indeed reduces the stochastic dependence of decryption failures. Therefore, the independence assumption gives a very close approximation to the true behavior of the cryptosystem. Second, we analyze and explore the influence of the LWE/RLWE parameters on the stochastic dependence. This exploration gives designers of LWE/RLWE based schemes the opportunity to compare different schemes with respect to the inaccuracy made by using the independence assumption. This work shows that the stochastic dependence depends on three LWE/RLWE parameters in different ways: i) it increases with higher lattice dimensions (n) and higher standard deviations of the error distribution ($\sqrt{k/2}$); and ii) it decreases with higher modulus (q).

Keywords: Lattice-based Cryptography · Stochastic Dependence · Correlation · Decryption Failure Rate.

1 Introduction

Post-Quantum cryptographic schemes based on the Learning with Errors (LWE) and the Ring-LWE (RLWE) problems exhibit a non-vanishing decryption failure rate. In order to decrease this failure rate without degrading the security level,

* G. Maringer and T. Fritzmann contributed equally to this work.

frequently Error-Correcting Codes (ECC) are used [5]. A low decryption failure rate does not only reduce the amount of re-transmissions but is also essential to avoid attacks which are capable to exploit these failures [4]. Therefore, a small decryption failure rate is desirable or in some settings even mandatory. The intuitive question is how to determine the decryption failure rate. The quantification of this failure rate is not straightforward due to the correlation between the coefficients of the noise term. Despite within RLWE schemes the coefficients of polynomials are sampled independently, their product does not keep the independent nature between the coefficients.

When no ECC is applied, simple inequalities, such as the Fréchet inequality, can be used to determine an upper bound of the overall decryption failure rate. For schemes that make use of an ECC, previous works assumed the coefficients to fail independently in order to compute the overall failure rate [11, 6]. However, the influence of the correlation on the failure rate and the validity of the independence assumption is still an open research question.

First discussions about the correlation were made in Hila5 [11], LAC [6], and [5]. In [3], it is shown that the influence of the correlation for the NIST submission LAC is larger than expected and therefore the failure rate was underestimated. The authors experimentally verified that the norms of certain polynomials are major contributors to the stochastic dependence. Conditioning the failure probabilities on these norms reduces the stochastic dependence on average. Assuming that the aforementioned averaged result also works for a single fixed norm, the LAC team decided to fix the norms to a specific value for the second round of the NIST competition. However, to the best of our knowledge, the influence of fixing the norms to a specific value on the stochastic dependence has not been analyzed so far. The constraint of fixing the norms significantly reduces the possible space of error polynomials. Therefore, stochastic independence when a specific value for the norms is chosen has to be analyzed. Moreover, previous works have not analyzed the influence of the RLWE parameters n (lattice dimensions), q (modulus), and k (related to the standard deviation of the error distribution) on the stochastic dependence of decryption failures.

In this work, we analyze the origin of the stochastic dependence of decryption failures and the effect of fixing the norms to their expected values. Moreover, we analyze the influence of the RLWE parameters on the applicability of the independence assumption. We introduce various measures for quantifying the stochastic dependence between random variables and statistically estimate them. The methods in this work are applied on RLWE schemes but are also suitable for LWE schemes.

2 Preliminaries

2.1 Notation

All polynomials in this paper are printed in bold and are an element of the ring $\mathcal{R} = \mathbb{Z}_q[x]/(x^n + 1)$, where n and q are both integers. The polynomials can be represented as $\boldsymbol{a} = \sum_{i=0}^{n-1} a_i x^i$, where all coefficients a_i are reduced after each operation modulo q. Let $a \overset{\$}{\leftarrow} S$ denote the sampling process from a distribution S. Let χ_k be a centered binomial distribution with standard deviation $\sigma = \sqrt{k/2}$. The norm of a polynomial is defined as $\|\boldsymbol{x}\|_2 := \sqrt{\sum_i x_i^2}$ and the norm of a vector of polynomials is defined as $\|\boldsymbol{Z}\|_2 := \sqrt{\sum_k \|\boldsymbol{z_k}\|_2^2}$. Let P_X be a distribution on a random variable X. Its support $\mathrm{supp}(P_X)$ denotes the set of all a such that $P_X(a) > 0$.

2.2 Ring Learning With Errors (RLWE)

The RLWE problem was introduced by Lyubashevsky *et al.* in [8] as a possibility of speeding up cryptographic constructions based on the LWE problem proposed by Regev in [10]. The hardness of this problem relies on recovering the secret polynomial $\boldsymbol{s}$ from $\boldsymbol{b} = \boldsymbol{a} \cdot \boldsymbol{s} + \boldsymbol{e}$, where the coefficients of the secret polynomial $\boldsymbol{s}$ and error polynomial $\boldsymbol{e}$ are usually sampled from a discrete Gaussian or a centered binomial distribution, and the coefficients of the public polynomial $\boldsymbol{a}$ from a large uniform distribution. Moreover, it is known to be a hard problem to distinguish $(\boldsymbol{a}, \boldsymbol{b})$ from a uniform sample in $\mathcal{R} \times \mathcal{R}$. RLWE instances are used as the main building blocks for several post-quantum cryptographic schemes.

2.3 Algorithmic Description

This subsection describes the general structure and basic principles of RLWE based schemes.

RLWE-based schemes are mainly defined by the parameters (n, q, k), where n determines the degree of the elements in $\mathcal{R}$, q is the modulus, and k determines the variance of the error distribution. The selection of the different parameter values creates different instances of the RLWE problem and influences the security level, key/ciphertext sizes, failure rate, and as we show in this work also the stochastic dependence between decryption failures.

A PKE/KEM system based on RLWE is composed of three major operations: key-generation, encryption and decryption. These operations are shown in Algorithm 1, Algorithm 2 and Algorithm 3, respectively.

The key generation creates the private key $sk = \boldsymbol{s}$ and the public key $pk = (\boldsymbol{b}, seed)$. It is composed of three steps. The first step generates the public polynomial $\boldsymbol{a}$ by using a cryptographic pseudo random number generator that is initialized with a truly random seed. All coefficients of $\boldsymbol{a}$ are uniformly distributed between 0 and $q - 1$. In the second step, the sampling of the secret polynomial $\boldsymbol{s}$ and the error polynomial $\boldsymbol{e}$ are performed. The coefficients of these polynomials are usually taken from a binomial distribution, which is centered at zero, having outcomes in $[-k, k] \mod q$. After the sampling process, in the third step, the RLWE instance $\boldsymbol{b} = \boldsymbol{as} + \boldsymbol{e}$ is computed.

During the encryption operation, any plaintext m is transformed into a ciphertext $c = (\boldsymbol{u}, \boldsymbol{v})$. It is composed of three steps. The first step generates the polynomial $\boldsymbol{a}$ as well as the secret and error polynomials $\boldsymbol{s'}$, $\boldsymbol{e'}$ and $\boldsymbol{e''}$. In the second step, before hiding the message m in the RLWE instance $\boldsymbol{v}$, the message is encoded into a polynomial. During this step, redundancy can be added to allow error correction after decryption. Finally, in the third step, the two RLWE instances $\boldsymbol{u}$ and $\boldsymbol{v}$ are created and can be sent securely over a public channel.

The decryption operation retrieves the hidden message m from c. It is composed of two steps. In the first step, the largest noise term $\boldsymbol{ass'}$ is removed from $\boldsymbol{v}$ by subtracting $\boldsymbol{us}$. In the second step, the ECC removes further errors. With high probability no decryption failure occurs and $\hat{m} = m$.

```
Algorithm 1: Key Generation
    $\text{seed} \xleftarrow{\$} \{0,1\}^{256}$
    $\boldsymbol{a} \leftarrow \text{GenA}(\text{seed})$
    $\boldsymbol{s}, \boldsymbol{e} \xleftarrow{\$} \chi_k$
    $\boldsymbol{b} \leftarrow \boldsymbol{a}\boldsymbol{s} + \boldsymbol{e}$
    Result: $pk = (\boldsymbol{b}, \text{seed})$, $sk = \boldsymbol{s}$
```

```
Algorithm 2: Encryption
    Input: $pk = (\boldsymbol{b}, \text{seed})$, $m \in \{0, \ldots, 255\}^{32}$
    $\boldsymbol{a} \leftarrow \text{GenA}(\text{seed})$
    $\boldsymbol{s'}, \boldsymbol{e'}, \boldsymbol{e''} \xleftarrow{\$} \chi_k$
    $\boldsymbol{u} \leftarrow \boldsymbol{a}\boldsymbol{s'} + \boldsymbol{e'}$
    $\boldsymbol{v} \leftarrow \boldsymbol{b}\boldsymbol{s'} + \boldsymbol{e''} + \text{Encode}(m)$
    Result: $c = (\boldsymbol{u}, \boldsymbol{v})$
```

```
Algorithm 3: Decryption
    Input: $c = (\boldsymbol{u}, \boldsymbol{v})$, $sk = \boldsymbol{s}$
    $\hat{m} \leftarrow \text{Decode}(\boldsymbol{v} - \boldsymbol{u}\boldsymbol{s})$
    Result: $\hat{m}$
```

3 Decryption Failures

As already indicated in Subsection 2.3, the efficient usage of an RLWE scheme has intrinsically a certain probability that the message m is not retrieved correctly after the decryption process. The large term $\boldsymbol{a}\boldsymbol{s}\boldsymbol{s'}$ in $\boldsymbol{v} - \boldsymbol{u}\boldsymbol{s} = \boldsymbol{e}\boldsymbol{s'} - \boldsymbol{e'}\boldsymbol{s} + \boldsymbol{e''} + \text{Encode}(m)$ cancels out and only a relatively small difference noise term remains additively on the encoded message

$$\boldsymbol{d} = \boldsymbol{e}\boldsymbol{s'} - \boldsymbol{e'}\boldsymbol{s} + \boldsymbol{e''} \ . \tag{1}$$

Another representation of this noise term is

$$\boldsymbol{d} = \boldsymbol{S}^T \boldsymbol{C} + \boldsymbol{G} \ , \tag{2}$$

where

$$\boldsymbol{S} = \begin{bmatrix} -\boldsymbol{s} \\ \boldsymbol{e} \end{bmatrix} \ , \quad \boldsymbol{C} = \begin{bmatrix} \boldsymbol{e'} \\ \boldsymbol{s'} \end{bmatrix} \ , \quad \boldsymbol{G} = \boldsymbol{e''} \ . \tag{3}$$

A coefficient fails if its absolute value $abs(d_i) > q_t$, where the threshold q_t is usually $q/4$ and d_i denotes the coefficients of $\boldsymbol{d}$. Throughout this work, the event of a failure in the i-th coefficient is denoted as F_i and a successful decryption is denoted as S_i. If an algebraic ECC is applied, up to t erroneous coefficients can be corrected, where t depends on the minimum distance of the code. The overall scheme fails when not all coefficients can be corrected. As a consequence, a retransmission of m might be necessary. The requirements for decryption failure rates depend on the application. For an ephemeral CPA-secure key exchange, a failure rate in the range of 2^{-40} might be acceptable because key agreement errors do not affect the security of the scheme [5]. However, CCA-secure PKE schemes require a much lower failure rate. Many schemes aim for failure rates that are lower than 2^{-128} (e.g., [2, 1]). The reason is that decryption failures can be exploited by an attacker as shown in [4].

4 The Stochastic Dependence Problem

The computation of the exact value of the failure rate of RLWE schemes turns out to be not straightforward. The reason is the stochastic dependence between the coefficients of the difference noise term $\boldsymbol{d}$, which emerges from the two polynomial multiplications $\boldsymbol{es'}$ and $\boldsymbol{e's}$.

In the past, for many algorithms based on the RLWE problem it was considered a valid assumption that the coefficients of $\boldsymbol{d}$ fail independently [11, 6, 5]. However, it was later shown that this is not the case in general. In [3], it was shown experimentally that the stochastic dependence between decryption failures for the parameters used in LAC leads to an overestimation of the security level. This effect has to be taken into account when choosing RLWE parameters.

4.1 Origin of the Stochastic Dependence

In this section, it is described why the stochastic dependence between coefficients of the polynomials within LWE/RLWE-based algorithms occurs.

Let $\boldsymbol{c} \in \mathcal{R}$ be the product of two polynomials $\boldsymbol{a}, \boldsymbol{b} \in \mathcal{R}$

$$\boldsymbol{c} = \boldsymbol{a} \cdot \boldsymbol{b} \mod (x^n + 1) \ . \tag{4}$$

The k-th coefficient of $\boldsymbol{c}$ is then given by

$$c_k = \sum_{i=0}^{k} a_i b_{k-i} - \sum_{i=k+1}^{n-1} a_i b_{n-i+k} \ . \tag{5}$$

A closer look at the first two coefficients of the product c_0 and c_1 already shows that there is a dependence between the coefficients.

$$c_0 = a_0 b_0 - a_1 b_{n-1} - a_2 b_{n-2} - a_3 b_{n-3} - \cdots - a_{n-1} b_1 \tag{6}$$

$$c_1 = a_0 b_1 + a_1 b_0 - a_2 b_{n-1} - a_3 b_{n-2} - \cdots - a_{n-1} b_2 \tag{7}$$

Note that both coefficients are composed from the same coefficients in $\boldsymbol{a}$ and $\boldsymbol{b}$, e.g., a_0 is used as a factor in the first product of each sum.

4.2 Influence of the Correlation on the Failure Rate

The calculation of the failure rate for a single coefficient can be determined exactly by convolving probability distributions in order to obtain the distribution of $d_i = (\boldsymbol{C}^T\boldsymbol{S} + \boldsymbol{G})_i$ as described in [5]. For LWE/RLWE schemes all coefficients have the same failure probability $p_b = P[|(\boldsymbol{C}^T\boldsymbol{S} + \boldsymbol{G})_i| > q/4]$. As described in Section 3, when more than t coefficients fail, where t is the number of correctable coefficients, the decryption fails. If no error correction is applied, simple inequalities, such as the Fréchet inequality, can be used to determine an upper bound of the overall failure rate. This bound does not require independent coefficients.

If the noise terms d_i would be independent, the failure rate could be exactly determined by

$$P[\boldsymbol{d}_f] = 1 - (1 - p_b)^n \ . \tag{8}$$

The problem of calculating the failure rate of the scheme gets more difficult when an ECC is applied. Current works assumed that the correlation between the coefficients is very low and has only a minor influence on the results [11, 7, 5]. This allows to calculate the overall failure rate for RLWE based systems that use an ECC by the formula

$$P[\boldsymbol{d}_f] = 1 - \sum_{i=0}^{t} \binom{n}{i} p_b^i (1 - p_b)^{n-i} \ . \tag{9}$$

4.3 Reducing the Stochastic Dependence

In [3] is stated that the main sources of the stochastic dependence of decryption failures are the norms of $\boldsymbol{S}$ and $\boldsymbol{C}$. They assumed that the decryption failures are independent conditioned on fixed values of $\|\boldsymbol{S}\|_2$ and $\|\boldsymbol{C}\|_2$.

If the decryption failures $F_0, \dots, F_{n-1}$ are assumed to be mutually independent conditioned on the norms of $\boldsymbol{S}$ and $\boldsymbol{C}$ the following equation holds:

$$P(F_0, \dots, F_{n-1} \mid \|\boldsymbol{S}\|_2, \|\boldsymbol{C}\|_2) = \prod_{i=0}^{n-1} P(F_i \mid \|\boldsymbol{S}\|_2, \|\boldsymbol{C}\|_2) \tag{10}$$

If this assumption would be not only an approximation but rather exact, fixing the norms of $\boldsymbol{S}$ and $\boldsymbol{C}$ would entirely remove the stochastic dependence between decryption failures.

In the first round submission of the NIST-PQC, LAC used the centered binomial distribution as the error distribution. This sampling is in the following referred to as Round 1 sampling. In order to sample a polynomial according to the error distribution, each coefficient is sampled independently and identically. As the independence assumption was experimentally shown not to be applicable in that case [3] and due to proposed low Hamming weight attacks [6], for the second round submission the amount of -1s, $+1$s and 0s in each error polynomial was fixed to their expected value according to the error distribution. This technique fixes its Hamming weight as well. This sampling is in the following referred to as Round 2 sampling.

Equation (10) is only an approximation and its applicability has only been checked experimentally averaged over all possible sets of norms of $\boldsymbol{S}$ and $\boldsymbol{C}$. However, for one specific norm-pair of $\boldsymbol{S}$ and $\boldsymbol{C}$ this has not been done so far. As a fixed norm-pair only occurs with small probability this step is essential.

5 Methods for Quantifying the Stochastic Dependence

The existence of a correlation between the coefficients after the polynomial multiplication is evident. However, it is unclear how strong this correlation is and how the parameters of LWE/RLWE schemes affect this phenomenon. In Subsection 5.1, the selection of the statistical approach to quantify the stochastic dependence between random variables is motivated. In Subsection 5.2 different measures for the stochastic dependence of random variables are introduced.

5.1 Statistical Estimation of Stochastic Dependence

The joint probability distribution of the product coefficients after the multiplication of two polynomials in $\mathcal{R}$ is unknown. To analytically compute this joint probability distribution is not straightforward, especially if various error distributions are considered. Fortunately, it is possible to estimate properties of random variables using statistical methods even if the respective random variable is unknown, e.g. the estimation of the expectation of a random variable X by taking the mean of N samples $(x_1, \dots, x_N)$

$$\overline{X} = \frac{1}{N} \sum_{k=1}^{N} x_k \tag{11}$$

which converges to the mean value if the variance of X is finite.

In this work, we propose a method which is based on statistical measurements as well. Our framework works for different kinds of error distributions. Therefore, we generate samples of $\boldsymbol{s}$, $\boldsymbol{e}$, $\boldsymbol{s'}$, $\boldsymbol{e'}$ and $\boldsymbol{e''}$ according to the error distribution. With each set of those samples the computation described in Eq. (1) is performed. Due to limited simulation time only the stochastic dependence between the first two coefficients of the result (d_0 and d_1) is considered for the measures discussed in Section 5.2. However, the ideas shown in this work can be extended to more than two coefficients.

We consider the random variables X and Y which map the respective values of d_0 and d_1 to the set $\{S, F\}$, where S denotes a successful decryption and F decryption failure. We formalize this for the random variable X. For Y, the formalism works accordingly.

$$X : \mathbb{Z}_q \to \{S, F\} \tag{12}$$

$$d_0 \mapsto \begin{cases} F, & \text{if } abs(d_0) > q_t \\ S, & \text{else} \end{cases} \tag{13}$$

This means that there are four events possible for the joint outcome of X and Y, F_0F_1, F_0S_1, S_0F_1 and S_0S_1. The first letter denotes the outcome of X and the second letter the outcome of Y. The joint probability distribution P_{XY} and the marginal distributions P_X and P_Y are estimated using histograms by measuring the occurrence the respective outcome and dividing it by the number of samples. The measures for stochastic dependence introduced in Section 5.2 are then computed from the estimated distributions.

5.2 Stochastic Dependence Calculation: Pearson Correlation, l_1-Distance and Mutual Information

The concept of stochastic independence is of major interest in probability theory. In this work, we are interested in measuring the amount of stochastic dependence between two random variables X and Y. It is crucial to find appropriate measures for stochastic dependence between random variables. In this section, we introduce three measures for stochastic dependence: Pearson correlation, l_1-distance, and mutual information.

The Pearson correlation coefficient measures the linear dependency between two random variables. It is defined by Eq. (14).

$$\rho(X,Y) := \frac{Cov(X,Y)}{\sqrt{Var(X)Var(Y)}} \tag{14}$$

Empirically the correlation coefficient is obtained by sampling long independent identically distributed sequences of the random variables X and Y and computing

$$r_{xy} := \frac{\sum_{i=0}^{n-1}(x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\sum_{i=0}^{n-1}(x_i - \overline{x})^2}\sqrt{\sum_{i=0}^{n-1}(y_i - \overline{y})^2}} \tag{15}$$

where $\overline{x} = \frac{1}{n}\sum_{i=0}^{n-1} x_i$ and $\overline{y} = \frac{1}{n}\sum_{i=0}^{n-1} y_i$.

The definition of the Pearson correlation coefficient only uses moments up to second order of the respective random variables. This means that even if the Pearson correlation between X and Y is zero the random variables are not necessarily independent. However, if X and Y are stochastically independent their Pearson correlation coefficient is zero.

Therefore, in the following alternative measures for stochastic dependence are presented. Perhaps the most intuitive measure is the l_1-distance, defined as

$$d(P_{XY}, P_X P_Y) := \|P_{XY} - P_X P_Y\|_1 = \sum_{a\in\mathcal{X}, b\in\mathcal{Y}} |P_{XY}(a,b) - P_X(a)P_Y(b)| \tag{16}$$

where $\mathcal{X}$ and $\mathcal{Y}$ denote the sets of possible outcomes of the random variables, P_{XY} their joint distribution and P_X, P_Y the marginal distributions of the random variables.

The definition already shows that two random variables X and Y are stochastically independent if and only if $d(P_{XY}, P_X P_Y) = 0$. As the distance between the joint distribution P_{XY} and the product of the marginal distributions $P_X P_Y$ is summed over all possible outcomes, the l_1-distance is an obvious candidate for a measure of stochastic dependence.

Another possible measure of stochastic dependence is mutual information. It was introduced by Shannon in [12] and shows similar properties to the l_1-distance. The mutual information $I(X;Y)$ is defined as

$$I(X;Y) := \sum_{(a,b)\in \mathrm{supp}\{P_{XY}\}} P_{XY}(a,b) \log_2\left(\frac{P_{XY}(a,b)}{P_X(a)P_Y(b)}\right) . \tag{17}$$

As for the l_1-distance, the mutual information between X and Y is 0 if and only if the random variables X and Y are stochastically independent. It is even mentioned as a potential measure for stochastic dependence in [9].

6 Experimental Results

Subsection 6.1 presents the influence of fixing the norm of the error distribution in LAC on the stochastic dependence of decryption failures. Subsection 6.2 shows the influence of the LWE/RLWE parameter sets (n, q, k) on the stochastic dependence of decryption failures. The analysis in this work is performed for the parameters used within the LAC-cryptosystem but the proposed methodology can be applied to any RLWE-based system.

6.1 Fixing the norm of the error distribution in LAC

Table 1 shows the failure probabilities, the absolute value of the Pearson correlation, the l_1-distance and the mutual information for LAC128 and LAC256. The results show a decrease of the failure probabilities for the sampling performed in the second round submission of LAC in the NIST-PQC . The statistical results for all previously introduced measures for stochastic dependence decrease for Round 2 sampling and therefore indicate less stochastic dependence.

Figure 1 and Fig. 2 show the maximal failure rate for a given error correction capability of the ECC for LAC128 and LAC256, respectively. Both figures show four different data sets: 1) theoretical results only assuming stochastic independence of decryption failures conditioned on the norms of $\boldsymbol{S}$ and $\boldsymbol{C}$ (method in [3]); 2) experimental results using Round 1 sampling of LAC; 3) theoretical results using the independence assumption; 4) experimental results using Round 2 sampling of LAC (fixed Hamming weight). The figures for both parameter sets show that the experimental results for Round 2 sampling perfectly match the theoretical results using the independence assumption. Therefore, we conclude that the stochastic dependence between decryption failures was significantly reduced compared to Round 1. This is in accordance with the results presented in Table 1. As a result, the independence assumption approximates the real behaviour of decryption failures significantly better for Round 2 sampling compared to Round 1 sampling. Therefore, we consider the independence assumption to be valid for Round 2 sampling.

Table 1. Results for LAC128 and LAC256 (1st/2nd Round), 10^{11} samples

Error distribution	**Pearson** (abs)	***l*1-distance**	**I**	$\mathbf{P}[F_0F_1]$	$\mathbf{P}[F_0S_1]$	$\mathbf{P}[S_0F_1]$	$\mathbf{P}[S_0S_1]$
LAC128 Round 1	8.852e-06	3.248e-09	5.477e-11	9.230e-09	9.170e-05	9.178e-05	0.99982
LAC128 Round 2	5.083e-06	1.805e-09	1.900e-11	7.430e-09	8.874e-05	8.879e-05	0.99982
LAC256 Round 1	1.032e-04	2.288e-06	7.546e-09	3.201e-05	5.575e-03	5.575e-03	0.98882
LAC256 Round 2	6.077e-06	1.347e-07	2.633e-11	3.143e-05	5.572e-03	5.572e-03	0.98882

6.2 Influence of the LWE Parameter Set (n, q, k) on the Stochastic Dependence

This subsection analyzes the influence of different RLWE parameters on the independence assumption. In this analysis, the centered binomial distribution is used as the error distribution. Figures 3, 4 and 5 depict the relation of (n, q, k) to the stochastic dependence of decryption failures. Experimentally determined curves deviate stronger from the curves using the independence assumption if the stochastic dependence between decryption failures is larger. In the following

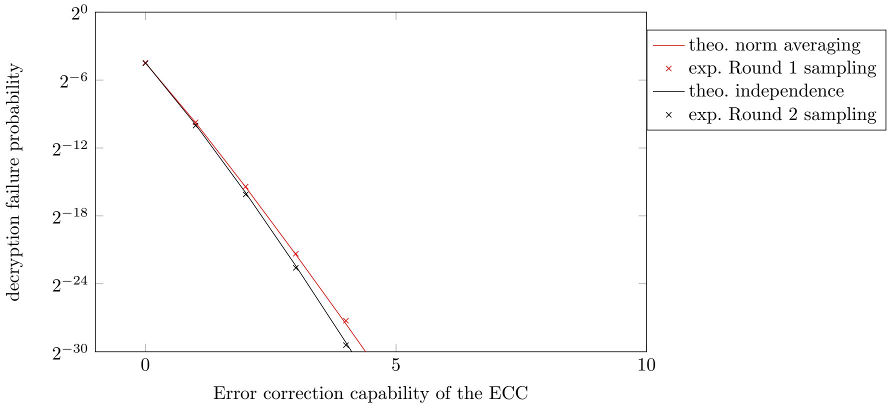

Fig. 1. Decryption failure probability depending on the error correction capability of the ECC (LAC-128)

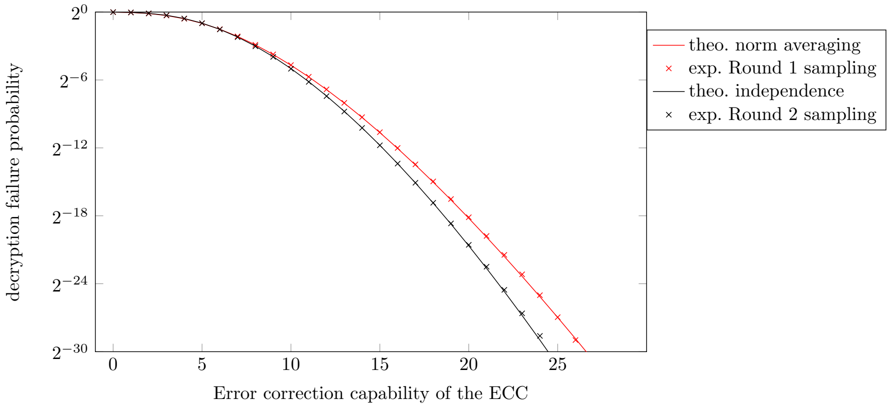

Fig. 2. Decryption failure probability depending on the error correction capability of the ECC (LAC-256)

LAC256 having $(n, q, k) = (1024, 251, 1)$ is used as a reference. Proceeding from this reference set each parameter has been varied to determine the respective parameter's influence on failure rate and stochastic dependence. In each figure, the experimentally determined decryption failure rates are compared with theoretical results obtained using the independence assumption. It is hard to analyze the influence of k for different values in LAC as its dependence on the failure probability is extremely high. Therefore, in Appendix A experiments for NewHope parameters with increased variance of the error distribution are depicted. In addition to Figures 3, 4 and 5, Table 2 shows the results obtained by the methods introduced in Section 5. Both results show that a higher decryption failure rate also leads to a larger deviation of the experimental data from the independence assumption. Therefore, larger values for n and k and smaller values for q increase the stochastic dependence of decryption failures and the independence assumption approximates the exact behaviour of decryption failures worse.

In the following, an explanation for this behaviour is given. As noted in Section 4.3 large norms of $\boldsymbol{S}$ and $\boldsymbol{C}$ increase the failure rate of RLWE based algorithms. The probability of obtaining large norms in $\boldsymbol{S}$ and $\boldsymbol{C}$ increases with larger n and k. The decryption failure rate increases with larger norms of $\boldsymbol{S}$ and $\boldsymbol{C}$ and decreases with larger q. A decryption failure can only occur if the norms of $\boldsymbol{S}$ and $\boldsymbol{C}$ are larger than a certain threshold which depends on q. Obtaining a decryption failure in one coefficient reduces the possible set of norms (and increases the probability for higher norms), which increases the chance of a decryption failure in other coefficients. Correct decryption of a coefficient in comparison only changes the probabilities of the norms of $\boldsymbol{S}$ and $\boldsymbol{C}$. Therefore, as shown in the figures the stochastic dependence between decryption failures increases with higher n and k and lower q. As a consequence the inaccuracy implied by using the independence assumption for computing the failure rate of a cryptographic scheme is higher for schemes which rely on strong ECCs to obtain a low decryption failure rate.

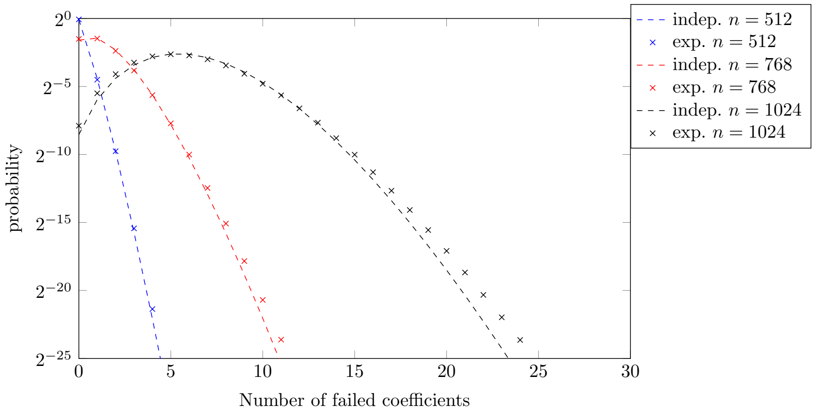

Fig. 3. Number of failed coefficients for fixed $q = 251$, and $k = 1$

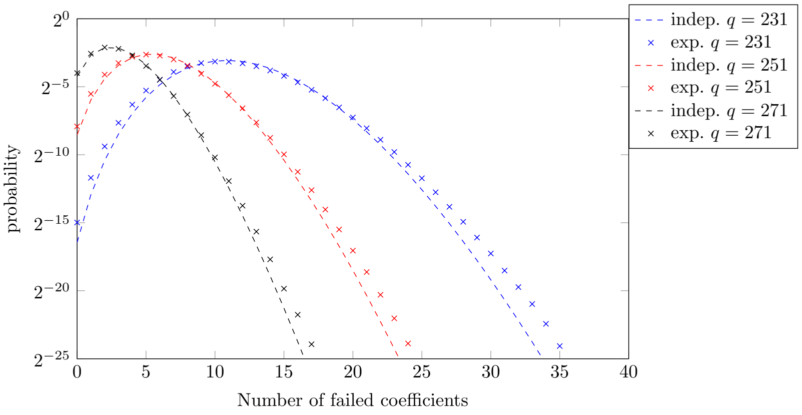

Fig. 4. Number of failed coefficients for fixed $n = 1024$, and $k = 1$

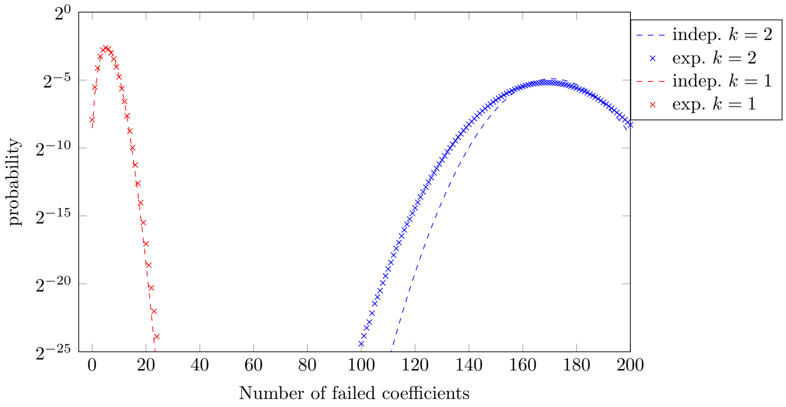

Fig. 5. Number of failed coefficients for fixed $n = 1024$, $q = 251$

Table 2. Pearson correlation, l_1-distance and mutual information for different parameter sets (n,q,k). 10^{11} samples, except for parameter set $(1024, 251, 2)$ - 10^9 samples, due to faster saturation of measures of stochastic dependence.

Parameter set	**Pearson** (abs)	***l*1-distance**	**I**	$\mathbf{P}[F_0F_1]$	$\mathbf{P}[F_0S_1]$	$\mathbf{P}[S_0F_1]$	$\mathbf{P}[S_0S_1]$
(**512**,251,1)	8.852e-06	3.248e-09	5.477e-11	9.230e-09	9.170e-05	9.178e-05	0.99982
(**768**,251,1)	5.445e-05	3.017e-07	2.105e-09	2.005e-06	1.387e-03	1.387e-03	0.99722
(**1024**,251,1)	1.032e-04	2.288e-06	7.546e-09	3.201e-05	5.575e-03	5.575e-03	0.98882
(1024,**231**,1)	1.414e-04	5.976e-06	1.406e-08	1.180e-04	1.068e-02	1.068e-02	0.97853
(1024,**251**,1)	1.032e-04	2.288e-06	7.546e-09	3.201e-05	5.575e-03	5.575e-03	0.98882
(1024,**271**,1)	6.897e-05	7.640e-07	3.384e-09	7.947e-06	2.777e-03	2.777e-03	0.99444
(1024,251,**1**)	1.032e-04	2.288e-06	7.546e-09	3.201e-05	5.575e-03	5.575e-03	0.98882
(1024,251,**2**)	5.063e-04	2.411e-04	1.371e-07	2.751e-02	0.13817	0.13817	0.69616

7 Conclusion

In this work, we analyzed the influence of the LWE/RLWE parameter set on the stochastic dependence between decryption failures caused by the difference noise term. To reduce the stochastic dependence between decryption failures in the second round LAC submission the Hamming weight of the error distribution was fixed. In this paper, the effect of fixing the Hamming weight on the stochastic dependence has been analyzed. Our results show that this measure achieves a significant decrease of the stochastic dependence between decryption failures. Therefore, if the error distribution chosen in the second round submission of LAC is used, assuming independence of decryption failures can be considered a valid simplification. Moreover, the results have shown that the standard deviation of the error distribution, the polynomials length, and the modulus all have a significant influence on this dependence. To quantify the stochastic dependence, the Pearson correlation, l_1-distance and mutual information between the failures of the individual coefficients were statistically determined. All those measures for stochastic dependence indicate that stochastic dependence increases with higher standard deviation, larger polynomial length, and smaller modulo reduction parameter. Although this work does not show an analytical solution to obtain the stochastic dependence between decryption failures, the proposed methods are suitable to compare different RLWE parameter sets.

Acknowledgments. G. Maringer's work was supported by the German Research Foundation (Deutsche Forschungsgemeinschaft, DFG) under Grant No. WA3907/4-1.

References

1. Alkim, E., Avanzi, R., Bos, J., Ducas, L., de la Piedra, A., Pöppelmann, T., Schwabe, P., Stebila, D.: NewHope: Algorithm Specifications And Supporting Documentation (2018), https://newhopecrypto.org/data/NewHope_2018_12_02.pdf
2. Avanzi, R., Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Schwabe, P., Seiler, G., Stehlé, D.: CRYSTALS-Kyber: Algorithm Specifications And Supporting Documentation (2019), https://www.pq-crystals.org/kyber/data/kyber-specification-round2.pdf
3. D'Anvers, J.P., Vercauteren, F., Verbauwhede, I.: The impact of error dependencies on ring/mod-lwe/lwr based schemes. Tech. rep., Cryptology ePrint Archive, Report 2018/1172 (2018)
4. Fluhrer, S.R.: Cryptanalysis of ring-lwe based key exchange with key share reuse. IACR Cryptology ePrint Archive **2016**, 85 (2016)
5. Fritzmann, T., Pöppelmann, T., Sepulveda, J.: Analysis of error-correcting codes for lattice-based key exchange. In: International Conference on Selected Areas in Cryptography. pp. 369–390. Springer (2018)
6. Lu, X., Liu, Y., Jia, D., Xue, H., He, J., Zhang, Z.: Supporting documentation: LAC (2017), https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-2-Submissions
7. Lu, X., Liu, Y., Jia, D., Xue, H., He, J., Zhang, Z.: Supporting documentation: LAC (2017), https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions
8. Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. In: Gilbert, H. (ed.) Advances in Cryptology – EUROCRYPT 2010. pp. 1–23. Springer Berlin Heidelberg, Berlin, Heidelberg (2010)
9. McEliece, R.: The theory of information and coding. Cambridge University Press (2002)
10. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: Proceedings of the Thirty-seventh Annual ACM Symposium on Theory of Computing. pp. 84–93. STOC '05, ACM, New York, NY, USA (2005). https://doi.org/10.1145/1060590.1060603, http://doi.acm.org/10.1145/1060590.1060603
11. Saarinen, M.J.O.: Supporting documentation: HILA5 (2017), https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions
12. Shannon, C.E.: A mathematical theory of communication. Bell system technical journal **27**(3), 379–423 (1948)

A Influence of k on the Stochastic Dependence

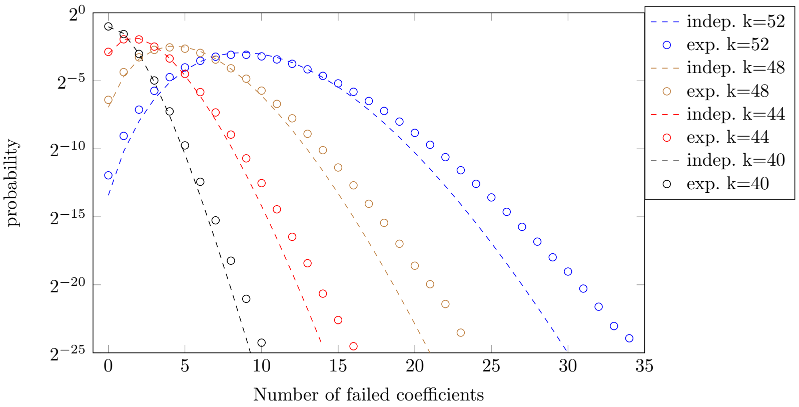

Fig. 6. Number of failed coefficients for fixed $n = 1024$, $q = 12289$

As mentioned in Subsection 6.2, NewHope parameters with an increased variance of the error distribution are used to show the influence of k on the stochastic dependence of decryption failures with finer granularity.

Figure 6 shows the influence of the variance of the error distribution on the probability of the number of decryption failures. The results show that increasing the variance increases the failure rate. It is also shown that the deviation between independence assumption and experimentally determined curves is increased for larger k.

Table 3 shows the Pearson correlation, $l1$-distance, and mutual information for $k = 40$ and $k = 52$. The results show an increase of the stochastic dependence when k is increased.

Table 3. Pearson correlation, l_1-distance and mutual information for different standard deviations of the error distribution ($1.8 \cdot 10^9$ samples)

Parameter set	**Pearson** (abs)	***l*1-distance**	**I**	$\mathbf{P}[F_0F_1]$	$\mathbf{P}[F_0S_1]$	$\mathbf{P}[S_0F_1]$	$\mathbf{P}[S_0S_1]$
1024,12289,40	8.931e-05	2.484e-07	5.514e-09	5.472e-07	6.956e-04	6.963e-04	0.99861
1024,12289,52	2.944e-04	1.047e-05	6.072e-08	8.460e-05	8.971e-03	8.969e-03	0.98198