Middle-Product Learning with Rounding Problem and its Applications

Shi Bai, Katharina Boudgoust, Dipayan Das, Adeline Roux-Langlois, Weiqiang Wen, Zhenfei Zhang

Middle-Product Learning with Rounding Problem and its Applications

Shi Bai[1], Katharina Boudgoust[2], Dipayan Das[3], Adeline Roux-Langlois[2], Weiqiang Wen[2], and Zhenfei Zhang[4]

[1] Department of Mathematical Sciences, Florida Atlantic University.
[2] Univ Rennes, CNRS, IRISA.
[3] Department of Mathematics, National Institute of Technology, Durgapur.
[4] Algorand.

Abstract. At CRYPTO 2017, Roşca et al. introduce a new variant of the *Learning With Errors* (LWE) problem, called the *Middle-Product* LWE (MP-LWE). The hardness of this new assumption is based on the hardness of the *Polynomial* LWE (P-LWE) problem parameterized by a set of polynomials, making it more secure against the possible weakness of a *single* defining polynomial. As a cryptographic application, they also provide an encryption scheme based on the MP-LWE problem. In this paper, we propose a deterministic variant of their encryption scheme, which does not need Gaussian sampling and is thus simpler than the original one. Still, it has the same quasi-optimal asymptotic key and ciphertext sizes. The main ingredient for this purpose is the *Learning With Rounding* (LWR) problem which has already been used to derandomize LWE type encryption. The hardness of our scheme is based on a new assumption called *Middle-Product Computational Learning With Rounding*, an adaption of the computational LWR problem over rings, introduced by Chen et al. at ASIACRYPT 2018. We prove that this new assumption is as hard as the decisional version of MP-LWE and thus benefits from worst-case to average-case hardness guarantees.

Keywords. LWE, LWR, Middle-Product, Public Key Encryption.

1 Introduction

Lattice-based cryptosystems attracted considerable research interest in recent years due to their versatility, assumed quantum-resilience and efficiency. The *Learning With Errors* problem, introduced by Regev [Reg05] in his pioneering work, serves as a fundamental computational problem in lattice-based cryptography. Informally, the LWE problem asks for the solution of a system of noisy linear modular equations: Given positive integers n and q, an LWE sample consists of $(\mathbf{a}, b = \langle \mathbf{a}, \mathbf{s} \rangle + e \bmod q)$ for a fixed vector $\mathbf{s} \in \mathbb{Z}^n$, where $\mathbf{a}$ is sampled from the uniform distribution over $\mathbb{Z}_q^n$ and e is sampled from a probability distribution χ over $\mathbb{R}$. The LWE problem exists in two versions: The *search* version asks to recover the secret $\mathbf{s}$ given arbitrarily many LWE samples; The *decision* version asks to distinguish between LWE samples and samples drawn from the uniform distribution over $\mathbb{Z}_q^n \times \mathbb{R}$.

As a very attractive property for cryptography, LWE enjoys worst-case to average-case reductions [Reg05,Reg09,Pei09,BLP$^+$13] from well-studied problems such as finding a set of short independent vectors (SIVP) or the decisional variant of finding short vectors (GapSVP) in Euclidean lattices. A standard conjecture is to assume that there is no polynomial-time algorithm that solves these problems (and their mildly approximated versions), even on quantum computers. Thus, any solver of the average-case problems can be transformed into a solver for any instance of the worst-case problem, which is presumed to be difficult.

The protocols relying on the hardness of LWE are inherently inefficient due to the size of the public keys which usually contain m elements of $\mathbb{Z}_q^n$, where m is the number of samples which is usually larger than $n\log(n)$. To improve the efficiency, structured variants of LWE have been proposed [SSTX09,LPR10,LS15]. One promising variant is the *Polynomial Learning With Errors* (P-LWE) problem, introduced by Stehlé et al. [SSTX09]. Given a monic irreducible polynomial $f \in \mathbb{Z}[x]$ and an integer $q \geq 2$, a P-LWE sample is given by $(a, b = a \cdot s + e \bmod q)$ for a fixed polynomial $s \in \mathbb{Z}_q[x]/f$, where a is sampled from the uniform distribution over $\mathbb{Z}_q[x]/f$ and e is sampled from a probability distribution χ over $\mathbb{R}[x]/f$. The P-LWE problem also admits worst-case to average-case connections from well-studied lattice problems. Whereas the hardness reductions for LWE start from the lattice problem in the class of general Euclidean lattices, the class has to be restricted to *ideal lattices* in the case of P-LWE. These ideal lattices correspond to the ideals in the polynomial ring $\mathbb{Z}[x]/f$. Lyubashevsky et al. [LPR10] propose another promising variant, namely the *Ring Learning With Errors* (R-LWE) problem, where polynomial rings are replaced by the ring of integers of some number fields. In the case of cyclotomic fields, the P-LWE and R-LWE problems coincide up to some parameter losses. As a recent result, Roşca et al. [RSW18] show that P-LWE and R-LWE are equivalent for a larger class of polynomials. In addition, they also investigate other relations between these structured variants.

Hedging against possible weak instances. Gaining in efficiency on the positive side comes with a potential decrease in the security level guarantees on the negative side. There are concrete examples of polynomials f for which the P-LWE becomes computationally easy: for instance when f has a linear factor over $\mathbb{Z}$ [CIV16]. Note that this case is excluded by restricting to irreducible polynomials. A review on the known weak instances of P-LWE and R-LWE is given by Peikert [Pei16]. To the best of our knowledge, it is still not fully understood how to choose a *good* polynomial for instantiating P-LWE.

Motivated by the question of how to choose a good polynomial, Lyubashevsky introduces the so-called $R^{<n}$-SIS problem [Lyu16], a variant of the *Short Integer Solution* (SIS) problem, whose hardness does not depend only on a *single* polynomial, but on a set of polynomials. Inspired by this, Roşca et al. [RSSS17] propose its LWE counterpart: the *Middle-Product Learning With Errors* (MP-LWE) problem. The MP-LWE problem is defined as follows: Taking two polynomials a and s over $\mathbb{Z}_q$ of degrees less than n and $n+d-1$, respectively, the middle-product $a \odot_d s$ is the polynomial of degree less than d given by the middle d

coefficients of $a \cdot s$. In other words, $a \odot_d s = \lfloor (a \cdot s \bmod x^{n+d-1})/x^{n-1} \rfloor$, where the floor rounding $\lfloor \cdot \rfloor$ denotes deleting all those terms with negative exponents on x. Instead of choosing a and s from the ring $\mathbb{Z}_q[x]/f$ as in the P-LWE setting, they are now elements of $\mathbb{Z}_q^{<n}[x]$ and $\mathbb{Z}_q^{<n+d-1}[x]$. Here, $\mathbb{Z}_q^{<n}[x]$ denotes the set of all polynomials with coefficients in $\mathbb{Z}_q$ of degree less than n for $n \geq 1$. For integers d, n and q with $q \geq 2$ and $0 < d \leq n$ as parameters, an MP-LWE sample is given by $(a, b = a \odot_d s + e \bmod q)$, where s is a fixed element of $\mathbb{Z}_q^{<n+d-1}[x]$, a is sampled from the uniform distribution over $\mathbb{Z}_q^{<n}[x]$ and e is sampled from a probability distribution χ over $\mathbb{R}^{<d}[x]$. As for the hardness of MP-LWE, Roşca et al. [RSSS17] establish a reduction from the P-LWE problem parametrized by a polynomial f to the MP-LWE problem defined independently of any such f. Thus, as long as the P-LWE problem defined over some f (belonging to a huge family of polynomials) is hard, the MP-LWE problem is also guaranteed to be hard. As a cryptographic application, Roşca et al. [RSSS17] propose a public-key encryption (PKE) scheme that is IND-CPA secure under the MP-LWE hardness assumption, with keys of size $\tilde{O}(\lambda)$ and running time $\tilde{O}(\lambda)$, where λ is the security parameter.

Learning With Rounding (LWR). In the worst-to-average case reduction of LWE [Reg05] and P-LWE [SSTX09] the error e is sampled from discrete Gaussian distributions. Such sampling procedure is in general costly, difficult to implement and vulnerable to side-channel attacks, e.g. [DB15,BHLY16,Pes16,Saa18]. In 2012, Banerjee et al. [BPR12] introduce a deterministic variant of LWE, namely the *Learning With Rounding* (LWR) problem. It is used to construct efficient pseudorandom functions [BPR12], lossy trapdoor functions and deterministic encryption schemes [AKPW13].

An LWR sample is given by $(\mathbf{a}, b = \lfloor \langle \mathbf{a}, \mathbf{s} \rangle \rceil_p)$, where $\mathbf{s} \in \mathbb{Z}_q^n$ is fixed and $\mathbf{a}$ is sampled from the uniform distribution over $\mathbb{Z}_q^n$. The rounding operator $\lfloor x \rceil_p$ denotes multiplying x by p/q and then rounding the result to the nearest integer modulo p. Informally, this rounding operator corresponds to dividing the set of elements of $\mathbb{Z}_q$ into p chunks, each containing approximately q/p elements. The definition can be adapted to a ring setting, denoted by R-LWR.

In the full version of their paper, published on the IACR Cryptology ePrint Archive, Banerjee et al. [BPR11] show a reduction from LWE to LWR with arbitrarily many samples, which also works for the ring counterpart. Unfortunately, the reduction requires q/p to be larger than the error size B (where B bounds the magnitude of the LWE error with high probability) by a super-polynomial factor, thus leading to a large modulus paired with a small error bound. This in turn implies that the underlying worst-case lattice-problems are assumed to be hard with super-polynomial approximation factors, which stands for a stronger assumption. In practice, this also leads to inefficient protocols.

Subsequent studies propose new reductions that work for a larger range of parameters. Alwen et al. [AKPW13] give a reduction that allows a polynomial modulus and modulus-to-error ratio. However, the modulus q in the reduction depends on the number of LWR samples, thus the number of samples needs to be fixed in prior by some polynomials. Further, the reduction imposes certain number theoretical restrictions on the modulus q. For example, power-of-two moduli are not covered. In a recent work, Bogdanov et al. [BGM$^+$16] use the Rényi divergence to show a sample preserving reduction. The reduction is also dimension preserving for the special case that the modulus is prime. They also provide a reduction from the search variant of R-LWE to the search variant of R-LWR. In another work, Alperin-Sheriff and Apon [AA16] further improve the parameter sets for the reduction. In particular, the reduction is dimension-preserving with a polynomial-sized modulus. However, the ring setting analogue, a reduction from decisional R-LWE to decisional R-LWR with a polynomial-sized modulus, is still an open problem. Nevertheless, due to the simplicity and efficiency of R-LWR, several schemes as SABER [DKRV18] and Round5 [BBF$^+$19] basing their hardness on R-LWR are currently participating in the NIST standardization process [NIS].

To overcome the lack of provable hardness for decisional R-LWR with practical parameters, Chen et al. [CZZ18] propose a new assumption, called the *Computational Learning With Rounding Over Rings* (R-CLWR) assumption. They show a reduction from decisional R-LWE to R-CLWR, where the secret in the R-LWE sample is drawn uniformly at random from the set of all invertible ring elements whose coefficients are small. They also show that one can construct an efficient PKE scheme based on the hardness of R-CLWR in the random oracle model.

Our contributions. Our first main contribution is a new hardness assumption which we refer to as the *Middle Product Computational Learning With Rounding* (MP-CLWR) problem. On the one hand, the MP-CLWR problem uses rounding in a similar way to R-LWR and hence avoids the error sampling. On the other hand, the MP-CLWR problem is analogue to the MP-LWE problem whose hardness does not depend on a specific polynomial. Thus, the MP-CLWR assumption enjoys the desired properties from both, the security advantage of MP-LWE and the simplicity advantage of LWR. We show that the MP-CLWR problem is at least as hard as the decisional MP-LWE problem parametrized over a set of polynomials (Section 4). To complete the reduction, we also bring in some new results on random Hankel matrices which might be of independent interest (Section 3). As a typical application, we propose a PKE scheme based on this MP-CLWR assumption which is IND-CPA secure in the random oracle model (Section 5). The attractiveness of our encryption scheme stems from the fact that we only have to round the middle-product of two polynomials instead of sampling Gaussian error during public key generation while guaranteeing the same security and having the same asymptotic key and ciphertext sizes as [RSSS17] (Section 6). Furthermore, we provide at the end of Section 6 a study of the concrete security of our scheme by looking at the currently best known attacks against it.

In the following, we give a brief overview of the MP-CLWR problem and our proof for its hardness. An MP-CLWR sample is given by $(a, b = \lfloor a \odot_d s \rceil_p)$, where a is sampled from the uniform distribution over $\mathbb{Z}_q^{<n}[x]$ and s is a fixed element in $\mathbb{Z}_q^{<n+d-1}[x]$. We define the MP-CLWR problem as the following game, where we embed the MP-CLWR samples into two experiments. In both experiments, three different parties appear: A challenger $\mathcal{C}$, an adversary $\mathcal{A}$ and a

source $\mathcal{S}$. The source $\mathcal{S}_1$ of the first experiment provides t different MP-CLWR samples $(a_i, \lfloor a_i \odot_d s \rceil_p)_{i \in [t]}$ and the source $\mathcal{S}_2$ of the second experiment provides t rounded uniform samples $(a_i, \lfloor b_i \rceil_p)_{i \in [t]}$, where all a_i and b_i are independently sampled from the corresponding uniform distribution. The challenger $\mathcal{C}$ now uses these samples to compute an Input and a Target. It sends the Input to the adversary $\mathcal{A}$ which itself computes an Output. The adversary wins the experiment if Target $=$ Output. The important point in this setting is that the challenger $\mathcal{C}$ and the adversary $\mathcal{A}$ are in both experiments the same. The MP-CLWR assumption captures that an adversary has no more advantage to compute the correct output if it receives rounded middle-product samples than if it gets rounded uniform samples. A formal definition of MP-CLWR is given in Section 4.1.

Our reduction from MP-LWE to MP-CLWR, shown in Theorem 2, is dimension-preserving and works for polynomial-sized modulus q. In more details, let d, n, p, q and t be positive integers with $0 < d \leq n$ and $q \geq p \geq 2$. The parameters d and n describe the order of the middle-product, t denotes the number of samples and p defines the rounding. Let χ be an error distribution over $\mathbb{R}^{<d}[x]$. We show the following sequence of reductions:

$$\begin{tikzcd}
\text{MP-LWE}_{q,n,d,\chi} \arrow[r, "\text{Lemma 11}"] \arrow[d, dashed] & \text{MP-LWE}^{\times}_{q,n,d,\chi} \arrow[d, "\text{Lemma 12}"] \\
\text{MP-CLWR}_{p,q,n,d,t} & \text{MP-CRLWE}_{p,q,n,d,t,\chi} \arrow[l, "\text{Lemma 13}"']
\end{tikzcd}$$

The first part of this sequence, Lemma 11, gives a reduction from decisional MP-LWE to decisional MP-LWE$^{\times}$, where the latter one denotes the MP-LWE problem where the secret is sampled uniformly at random from the set of elements having full rank Hankel matrix. The Hankel matrix plays an important role during the reductions as one can use it to represent the middle-product. In Section 3 we prove new results on random Hankel matrices, which might be of independent interest. We give a lower bound of the probability that the Hankel matrix of a random element has full rank and prove a uniformity property of the middle-product. This property is used in Lemma 13, where we show a reduction from the rounded middle-product LWE problem to the middle-product LWR problem, for their computational versions. Note that using the Rényi divergence asks for fixing the requested number of samples t a priori. This is a necessary requirement which is also imposed in [BGM^{+}16] and [CZZ18].

Similarly to the encryption scheme of Chen et. al [CZZ18], we make use of the reconciliation mechanism of Peikert [Pei14]. In order to show the correctness of our scheme, we have to guarantee that the reconciliation method succeeds. We also use a probabilistic lifting function to lift elements from $\mathbb{Z}_p[x]$ to elements in $\mathbb{Z}_q[x]$. To prove the IND-CPA security of our scheme, we use the general leftover hash lemma from [RSSS17]. We show that a lifted version of their family of hash functions is still universal (Lemma 8).

Open Problems. As mentioned above, a reduction from decisional R-LWE to decisional R-LWR with a polynomial-sized modulus is still an open problem.

This carries over to the middle-product setting, where it would also be of interest to show a reduction from decisional MP-LWE to decisional MP-LWR. Such a hardness result would help to build a secure encryption scheme based on the decisional MP-LWR in the standard model. A search-to-decision reduction for R-LWR or MP-LWR would be an alternative way to promise the security of such protocols.

2 Preliminaries

Let q be a positive integer, then $\mathbb{Z}_q$ denotes the ring of integers modulo q. For any natural number n, we represent the set $\{1, \ldots, n\}$ by $[n]$. In order to ease readability, a vector $\mathbf{a}$ will be denoted in a bold small letter and a matrix $\mathbf{A}$ in a bold capital letter. By $\mathbf{a}^t$ and $\mathbf{A}^t$ we denote the transpose of the vector $\mathbf{a}$ and the matrix $\mathbf{A}$, respectively. For a positive integer n, we write $\mathbb{Z}^{<n}[x]$ to describe the set of all polynomials in $\mathbb{Z}[x]$ with degree less than n. We identify each polynomial a in $\mathbb{Z}^{<n}[x]$ with its coefficient column vector $\mathbf{a} = (a_0, \ldots, a_{n-1})^t$. Further, we denote by $\overline{\mathbf{a}}$ its coefficient vector in reverse order, hence $\overline{\mathbf{a}} = (a_{n-1}, \ldots, a_0)^t$. For any n-dimensional vector $\mathbf{a}$, we set the infinity norm $\|\mathbf{a}\|_\infty = \max_{i\in[n]} |a_i|$ and the Euclidean norm $\|\mathbf{a}\|_2 = \sqrt{\sum_{i\in[n]} a_i^2}$. If the index range is clear from the context, we will write $(a_i)_i$ instead of $(a_i)_{i\in[n]}$.

2.1 Rounding

Let p and q be integers both larger than 1. We define the *modular rounding function* $\lfloor\cdot\rceil_p : \mathbb{Z}_q \to \mathbb{Z}_p$ as $\lfloor x \rceil_p = \left\lfloor \left(\frac{p}{q}\right) \cdot x \right\rceil \bmod p$. The rounding function extends component-wise to vectors over $\mathbb{Z}_q$ and coefficient-wise to polynomials in $\mathbb{Z}_q[x]$. Note that we use the same notation as Banerjee et al. [BPR12] for the purpose of coherence. It is also possible to use the floor rounding function $\lfloor\cdot\rfloor$, where each element is rounded down to the next smaller integer, as for instance done by Chen et al. [CZZ18].

2.2 Reconciliation

Reconciliation is a method used by two parties to agree on a secret bit, where they only share a common value up to an approximation factor. A first reconciliation mechanism was presented by Ding et al. [DXL12] followed by other proposals (e.g., [Pei14,ADPS16]). We use the notation of Peikert and exert the nearest integer rounding. For this purpose, we need the rounding function $\lfloor\cdot\rceil_2 : \mathbb{Z}_q \to \mathbb{Z}_2$ for $p = 2$ and define the *reconciliation cross-rounding function* $\langle\cdot\rangle_2 \colon \mathbb{Z}_q \to \mathbb{Z}_2$ as

$$\langle x \rangle_2 = \left\lfloor \left(\frac{4}{q}\right) \cdot x \right\rceil \bmod 2.$$

For q even, the reconciliation algorithm `REC` takes as input two values $y \in \mathbb{Z}_q$ and $b \in \{0, 1\}$ and outputs $\lfloor x \rceil_2$, where x is the closest element to y such that $\langle x \rangle_2 = b$. A concrete definition of $\mathtt{REC}$ is given as follows. Define two disjoint intervals $I_0 = \{0, \dots, \lfloor \frac{q}{4} \rceil - 1\}$ and $I_1 = \{-\lfloor \frac{q}{4} \rfloor, \dots, -1\}$. Let E be the set given by $[-\frac{q}{8}, \frac{q}{8}) \cap \mathbb{Z}$. Further, let y be an element of $\mathbb{Z}_q$ and b be a bit. Then,

$$\mathtt{REC}(y, b) = \begin{cases} 0\,, & y \in I_b + E \bmod q, \\ 1\,, & \text{else.} \end{cases}$$

We recall the following results about the cross-rounding function and the reconciliation mechanism from Peikert [Pei14].

Lemma 1. *For q even, if $x \in \mathbb{Z}_q$ is uniformly random, then is $\lfloor x \rceil_2$ uniformly random given $\langle x \rangle_2$.*

Lemma 2. *For q even and $x, y \in \mathbb{Z}_q$ such that $|x - y| < \frac{q}{8}$, then*

$$\mathtt{REC}(y, \langle x \rangle_2) = \lfloor x \rceil_2\,.$$

In the case of q odd, thus $2 \nmid q$, the output bit of the reconciliation method is biased. That is why Peikert [Pei14] introduced a randomized doubling function

$$\mathtt{DBL}\colon \mathbb{Z}_q \to \mathbb{Z}_{2q}, \quad \mathtt{DBL}(x) = 2x - e,$$

where $e \leftarrow \{-1, 0, 1\}$ with probabilities $p_{-1} = p_1 = \frac{1}{4}$ and $p_0 = \frac{1}{2}$.

Lemma 3. *For q odd, if $x \in \mathbb{Z}_q$ is uniformly random, $\overline{x} \leftarrow \mathtt{DBL}(x)$, then is $\lfloor \overline{x} \rceil_2$ uniformly random given $\langle \overline{x} \rangle_2$.*

Lemma 4. *For q odd and $x, y \in \mathbb{Z}_q$ such that $|x - y| < \frac{q}{8}$, let $\overline{x} \leftarrow \mathtt{DBL}(x)$, then*

$$\mathtt{REC}(y, \langle \overline{x} \rangle_2) = \lfloor \overline{x} \rceil_2\,.$$

We extend all functions $\langle \cdot \rangle_2$, $\lfloor \cdot \rceil_2$ and $\mathtt{DBL}(\cdot)$ component-wise to vectors over $\mathbb{Z}_q$ and coefficient-wise to polynomials in $\mathbb{Z}_q[x]$, as well as the mechanism $\mathtt{REC}$ to vectors over $\mathbb{Z}_q \times \{0,1\}$ and to polynomials in $\mathbb{Z}_q[x] \times \{0,1\}[x]$.

Let p and q be integers such that $2 \leq p \leq q$. We define a probabilistic lifting function $\mathtt{INV}(\cdot)\colon \mathbb{Z}_p \to \mathbb{Z}_q$ that takes $x \in \mathbb{Z}_p$ as input and chooses uniformly at random an element u from the set $\{u \in \mathbb{Z}_q \colon \lfloor u \rceil_p = x\}$. As usual, $\mathtt{INV}(\cdot)$ can be extended coefficient-wise to $\mathbb{Z}_q^{<n}[x]$. This lifting function becomes important in the encryption scheme in Section 5. There, we use $\mathtt{INV}(\cdot)$ to lift rounded polynomials in $\mathbb{Z}_p[x]$ to $\mathbb{Z}_q[x]$ such that $\left\lfloor \mathtt{INV}(\lfloor a \rceil_p) \right\rceil_p = \lfloor a \rceil_p$. Note that $\mathtt{INV}(\lfloor a \rceil_p) = a + e$ with $\|e\|_\infty \leq \frac{q}{p}$.

2.3 Probabilities

For a set S and a distribution χ over S, we denote by $x \leftarrow \chi$ the process of sampling $x \in S$ according to χ. With $x \leftarrow U(S)$ we denote sampling x according to the uniform distribution over S. In this work, the support S is sometimes a subset of $\mathbb{R}$. In such a case, we say a distribution χ is *B-bounded with probability at least δ* for a real number $B \geq 0$, if $\Pr_{x \leftarrow \chi}[|x| \leq B] \geq \delta$. We say a B-bounded distribution χ is *balanced* if $\Pr_{x \leftarrow \chi}[|x| \leq 0] \geq \frac{1}{2}$ and at the same time $\Pr_{x \leftarrow \chi}[|x| \geq 0] \geq \frac{1}{2}$. For the parameter $s > 0$, we define the *Gaussian function* $\rho_s \colon \mathbb{R}^n \to (0,1]$ as $\rho_s(x) = \exp(-\pi \langle x, x \rangle / s^2)$. Normalizing this function yields the density function of the *continuous Gaussian distribution* D_s of standard deviation s. A (finite) family H of hash functions $h \colon X \to Y$ is called *universal* if

$$\Pr_{h \leftarrow U(H)} \left[h(x_1) = h(x_2) \right] = \frac{1}{|Y|},$$

for all $x_1 \neq x_2 \in X$. Roşca et al. [RSSS17] introduced the following variant of the leftover hash lemma.

Lemma 5 (Generalized Leftover Hash Lemma). *Let X, Y and Z be finite sets, H be a universal family of hash functions $h \colon X \to Y$ and $f \colon X \to Z$ be an arbitrary function. Then, for any random variable T taking values in X we have*

$$\varDelta \left((h, h(T), f(T)), (h, U(Y), f(T)) \right) \leq \frac{1}{2} \cdot \sqrt{\gamma(T) \cdot |Y| \cdot |Z|},$$

where $\gamma(T) = \max_{t \in X} \Pr \left[T = t \right]$.

Definition 1 (Statistical distance) *Let P and Q be two discrete probability distributions on a discrete domain E. Their* statistical distance *is defined as*

$$\varDelta(P; Q) = \frac{1}{2} \sum_{x \in E} |P(x) - Q(X)|.$$

The *Rényi divergence* [R6́1,vEH14] defines another measure of distribution closeness and was first used in cryptography as a powerful alternative for the statistical distance measure by Bai et al. [BLL+15]. In this paper, it suffices to use the Rényi divergence of order 2.

Definition 2 (Rényi divergence of order 2) *Let P and Q be two discrete probability distributions such that* $\mathrm{Supp}(P) \subset \mathrm{Supp}(Q)$. *The* Rényi divergence of order 2 *is defined as*

$$\mathrm{RD}_2(P \| Q) = \sum_{x \in \mathrm{Supp}(P)} \frac{P(x)^2}{Q(x)}.$$

The Rényi divergence admits the following properties, proved in [vEH14].

Lemma 6. *Let P, Q be two discrete probability distributions with* $\mathrm{Supp}(P) \subset \mathrm{Supp}(Q)$. *Further, let $(P_i)_i, (Q_i)_i$ be two families of independent discrete probability distributions with* $\mathrm{Supp}(P_i) \subset \mathrm{Supp}(Q_i)$ *for all i. Then, the following properties are fulfilled:*

1. ***(Data Processing Inequality)*** $\mathrm{RD}_2(P^f \| Q^f) \leq \mathrm{RD}_2(P\|Q)$ *for any function f, where P^f (resp. Q^f) denotes the distribution of $f(y)$ induced by sampling $y \leftarrow P$ (resp. $y \leftarrow Q$),*
2. ***(Multiplicativity)*** $\mathrm{RD}_2\left(\prod_i P_i \| \prod_i Q_i\right) = \prod_i \mathrm{RD}_2(P_i \| Q_i)$*,*
3. ***(Probability Preservation)*** *Let $E \subset \mathrm{Supp}(Q)$ be an arbitrary event, then*
$$Q(E) \cdot \mathrm{RD}_2(P\|Q) \geq P(E)^2.$$

2.4 Middle-Product Learning With Errors

The use of the middle-product in lattice-based cryptography was introduced by Roşca et al. [RSSS17] in the form of the so-called *Middle-Product Learning With Errors* (MP-LWE) problem.

Definition 3 (Middle-Product) *Let d_a, d_b, d, k be integers fulfilling the equation $d_a + d_b - 1 = d + 2k$. The middle-product of $a \in \mathbb{Z}^{<d_a}[x]$ and $b \in \mathbb{Z}^{<d_b}[x]$ is defined as*
$$a \odot_d b = \left\lfloor \frac{a \cdot b \bmod x^{k+d}}{x^k} \right\rfloor,$$
where the floor rounding in this case means removing all terms with negative exponents on x.

The middle-product fulfills additivity if one of its inputs is fixed. Associativity is generally not achieved, instead only the following weaker associativity property is guaranteed.

Lemma 7. *Let d, k and n be positive integers. For all $r \in \mathbb{Z}^{<k+1}[x]$, $a \in \mathbb{Z}^{<n}[x]$ and $s \in \mathbb{Z}^{<n+d+k-1}[x]$, we have*
$$r \odot_d (a \odot_{d+k} s) = (r \cdot a) \odot_d s.$$

In order to prove the security of the encryption scheme in Section 5, we need the following hash function family to be universal. Recall that $\mathtt{INV}(\cdot)$ denotes the probabilistic lifting function from $\mathbb{Z}_p[x]$ to $\mathbb{Z}_q[x]$ for two integers p and q with $2 \leq p \leq q$.

Lemma 8. *Let q, k, d, p and t be integers such that $k, d \geq 2$ and $2 \leq p \leq q$. For $(b_i)_{i\in[t]} \in (\mathbb{Z}_p^{<d+k}[x])^t$, we define*
$$h_{(b_i)_i} \colon \left(\{0,1\}^{<k+1}[x]\right)^t \to \mathbb{Z}_q^{<d}[x]$$
to be the map that sends
$$(r_i)_i \mapsto \sum_{i\in[t]} \mathtt{INV}(b_i) \odot_d r_i.$$
The hash function family $(h_{(b_i)_i})_{(b_i)_i}$ is universal.

Proof. The proof is very similar to the one of [RSSS17, Lemma 4.2]. We simply replace b_i by $\texttt{INV}(b_i)$, using the same argument to show that

$$\Pr_{(b_i)_i \leftarrow U\left((\mathbb{Z}_p^{<d+k}[x])^t\right)} \left[\sum_{i \in [t]} \texttt{INV}(b_i) \odot_d r_i = \sum_{i \in [t]} \texttt{INV}(b_i) \odot_d r_i' \right] = \frac{1}{q^d},$$

with $(r_i)_i \neq (r_i')_i$. □

We now recall the Learning With Errors (LWE) problem in the polynomial and middle-product setting, together with the hardness result of the latter one. The reader is referred to the original paper by Roşca et al. [RSSS17] for more details.

Definition 4 (Decisional P-LWE) *Let q and m be integers fulfilling $q \geq 2$ and $m > 0$. Let f be a polynomial in $\mathbb{Z}[x]$ of degree m and χ be a distribution over $\mathbb{R}[x]/f$. The decisional* $\text{P-LWE}^f_{q,\chi}$ *problem asks to distinguish arbitrary many samples of the form $(a_i, b_i = a_i \cdot s + e_i \bmod q)$, where $e_i \leftarrow \chi$ and $a_i \leftarrow U(\mathbb{Z}_q[x]/f)$, from the same number of samples chosen uniformly from $\mathbb{Z}_q[x]/f \times \mathbb{R}_q[x]/f$ with non-negligible success probability over the choices of $s \leftarrow U(\mathbb{Z}_q[x]/f)$.*

Definition 5 (Decisional MP-LWE) *Let q, d and n be integers with $q \geq 2$ and $0 < d \leq n$. Further, let χ be a distribution over $\mathbb{R}^{<d}[x]$. The decisional* $\text{MP-LWE}_{q,n,d,\chi}$ *problem asks to distinguish arbitrary many samples of the form $(a_i, b_i = a_i \odot_d s + e_i \bmod q)$ where $e_i \leftarrow \chi$ and $a_i \leftarrow U(\mathbb{Z}_q^{<n}[x])$, from the same number of samples chosen uniformly from $\mathbb{Z}_q^{<n}[x] \times \mathbb{R}_q^{<d}[x]$ with non-negligible success probability over the choices of $s \leftarrow U(\mathbb{Z}_q^{<n+d-1}[x])$.*

If instead the secret s is chosen uniformly at random from the set of all elements in $\mathbb{Z}_q^{<n+d-1}[x]$ having a Hankel matrix (see Section 3) of order $d+n-1$ of full rank d, denoted by $s \leftarrow U\left((\mathbb{Z}_q^{<n+d-1}[x])^\times\right)$, we call the corresponding problem $\text{MP-LWE}^\times_{q,n,d,\chi}$. Note that the main difference is the imposed full-rank condition, which plays an important role in Section 4.

Theorem 1 (Hardness of MP-LWE [RSSS17, Thm. 3.6]). *Let q, d and n be integers with $0 < d \leq n$ and $q \geq 2$. Further, let $\alpha \in (0,1)$. For $S > 0$, let $\mathcal{F}(S,d,n)$ denote the set of all monic polynomials f in $\mathbb{Z}[x]$ whose constant coefficient is coprime to q, having degree $m \in [d,n]$ and $\text{EF}(f) < S$. Then, there exists a probabilistic polynomial-time reduction from* $\text{P-LWE}^f_{q,D_{\alpha q}}$ *for any polynomial $f \in \mathcal{F}(S,d,n)$ to* $\text{MP-LWE}_{q,n,d,D_{\alpha' q}}$ *with $\alpha' = \alpha d S$.*

Recall that $D_{\alpha q}$ (resp. $D_{\alpha' q}$) denotes the Gaussian distribution of width αq (resp. $\alpha' q$). Further, $\text{EF}(f)$ is the expansion factor of f, introduced by Lyubashevsky and Micciancio [LM06] and defined as

$$\text{EF}(f) = \max\left(\frac{\|g \bmod f\|_\infty}{\|g\|_\infty} : g \in \mathbb{Z}^{2m-1}[x] \setminus \{0\} \right).$$

3 Random Hankel Matrices

In this section, we show new results on the distribution of random Hankel matrices. First, we recall the definition of Hankel and Toeplitz matrices for a given polynomial, which we interpret as usual as a vector. We prove a lower bound for the probability that the Hankel matrix of a polynomial which is chosen uniformly at random has full rank. Finally, this result leads to a uniformity property of the middle-product which plays a crucial part in the hardness reduction of the new middle-product learning with rounding assumption in Section 4.2.

Hankel and Toeplitz matrices are not only used in the context of the middle-product of two polynomials. More generally, as pointed out by Kaltofen and Lobo [KL96], Toeplitz matrices are used as pre-conditioners in the process of solving linear systems of equations having unstructered coefficient matrices. The attractiveness of these structured matrices is twofold: First, it suffices to store the first column and first row, in order to rebuild the whole matrix. Second, the product of a Toeplitz matrix and a vector is in fact a convolution and can be computed in superlinear time using the fast Fourier transformation.

Other than that, large-dimensional random matrices with additional algebraic structure, as Hankel and Toeplitz matrices, play an important role in statistics, in particular in multivariate analysis. More concretely, Hankel matrices arise in polynmoial regressions and Toeplitz matrices appear as covariance of stationary processes. In particular, the spectral distribution for their eigenvalues is important and was studied by Bryc et al. [BDJ06].

Let q be any positive integer and $a \in \mathbb{Z}_q^{<n+d-1}[x]$ be a polynomial over $\mathbb{Z}_q$ with coefficient vector $\mathbf{a} = (a_0, \ldots, a_{n+d-2})^t$. We define the *Hankel matrix* of a of *order* $d + n - 1$ as

$$\mathbf{Hank}(a) = \begin{pmatrix} a_0 & a_1 \ldots & a_{d-1} & \ldots & a_{n-1} \\ a_1 & a_2 \ldots & a_d & \ldots & a_n \\ & \iddots & & \vdots & \\ a_{d-1} & a_d \ldots & a_{2d-2} & \ldots & a_{n+d-2} \end{pmatrix} \in \mathbb{Z}_q^{d \times n}.$$

The Hankel matrix is fully determined by its first row and its last column. Its rank is at most d. If it has full rank d we write $\mathrm{rank}(\mathbf{Hank}(a)) = d$. Further, we recall the definition of Toeplitz matrices. Let $a \in \mathbb{Z}_q^{<n+d-1}[x]$ be a polynomial over $\mathbb{Z}_q$ with coefficient vector $\mathbf{a} = (a_0, \ldots, a_{n+d-2})^t$. The *Toeplitz matrix* of a of *order* $d + n - 1$ is given by

$$\mathbf{Toep}(a) = \begin{pmatrix} a_0 & a_1 & a_2 & \ldots & \ldots & a_{n-1} \\ a_n & a_0 & a_1 & \ddots & & \vdots \\ a_{n+1} & a_n & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & a_1 & a_2 \\ \vdots & & \ddots & a_n & a_0 & a_1 \\ a_{n+d-2} & \ldots & \ldots & a_{n+1} & a_n & a_0 \end{pmatrix} \in \mathbb{Z}_q^{d \times n}.$$

The Toeplitz matrix is fully determined by its first row and its first column. There exists a special relation between the Toeplitz matrix and the Hankel matrix. Let $\mathbf{J}_n$ be the reflection matrix of order n defined as

$$\mathbf{J}_n = \begin{pmatrix} 0 \cdots 0\, 0\, 1 \\ 0 \cdots 0\, 1\, 0 \\ 0 \cdots 1\, 0\, 0 \\ \vdots \;\iddots\; \vdots \; \vdots \; \vdots \\ 1 \cdots 0\, 0\, 0 \end{pmatrix} \in \mathbb{Z}_q^{n \times n}.$$

Then, for any polynomial $a \in \mathbb{Z}_q^{<n+d-1}[x]$ with coefficient vector $\mathbf{a} = (\mathbf{a}', \mathbf{a}'')$ in $\mathbb{Z}_q^n \times \mathbb{Z}_q^{d-1}$ it yields $\mathbf{Toep}(a) \cdot \mathbf{J}_n = \mathbf{Hank}(\tilde{a})$, where $\tilde{a}$ is the polynomial given by the coefficient vector $\tilde{\mathbf{a}} = (\overline{\mathbf{a}'}, \mathbf{a}'')$ with $\overline{\mathbf{a}'}$ denoting the vector $\mathbf{a}'$ in reverse order. Thus, we can use the result of Kaltofen and Lobo [KL96] about random Toeplitz matrices to calculate the probability of a random Hankel matrix to have full rank.

Lemma 9. *Let q be a positive integer with unique prime power factorization given by $q = \prod_{i \in [l]} p_i^{\alpha_i}$, where p_i are primes and $\alpha_i > 0$. Let d and n be integers with $0 < d \leq n$ and choose $b \leftarrow U(\mathbb{Z}_q^{<n+d-1}[x])$. Then,*

$$\Pr\left[\operatorname{rank}(\mathbf{Hank}(b)) = d\right] \geq \prod_{i \in [l]} \left(1 - \frac{1}{p_i}\right).$$

Proof. Case 1 (q is prime). Any Hankel matrix of order $d + n - 1$ can be represented as the matrix product of the corresponding Toeplitz matrix of order $d + n - 1$ times the non-singular reflection matrix $\mathbf{J}_n$ of order n whose anti-diagonal elements are 1's and all other entries are 0's. Thus, the rank of a given Hankel matrix will be the same as the one of the corresponding Toeplitz matrix. For the case $d = n$, it follows from Theorem 4 of [KL96] that the total number of Hankel matrices of full rank d is exactly $(q-1)q^{2d-2}$. If we choose $b \leftarrow U(\mathbb{Z}_q^{<n+d-1}[x])$, then

$$\Pr\left[\operatorname{rank}(\mathbf{Hank}(b)) = d\right] = \frac{(q-1)q^{2d-2}}{q^{2d-1}} = 1 - \frac{1}{q}.$$

For $d < n$, the $d \times n$ Hankel matrix has full rank d if at least the left $d \times d$ submatrix, which is naturally a $d \times d$ Hankel matrix as well, has rank d. This happens with probability at least $1 - \frac{1}{q}$.

Case 2 ($q = p^\alpha$). Initially, consider the case $d = n$. Any Hankel matrix $\mathbf{A}$ can be represented as $\mathbf{A} = p\mathbf{Q} + \mathbf{R}$, where both $\mathbf{R}$ and $\mathbf{Q}$ are Hankel matrices with coefficients in $\mathbb{Z}_p$ and $\mathbb{Z}_{p^{\alpha-1}}$, respectively. This formula follows from integer division by p with remainder, i.e., Euclidean division. Any element from $\mathbb{Z}_{p^\alpha}$, when divided by p, has a reminder in $\mathbb{Z}_p$ and quotient in $\mathbb{Z}_{p^{\alpha-1}}$. This representation is unique, thus preserves the structure of the matrix $\mathbf{A}$. Since $\mathbf{A}$ is a

Hankel matrix, so are $\mathbf{Q}$ and $\mathbf{R}$. The matrix $\mathbf{A}$ has full rank in $\mathbb{Z}_{p^\alpha}$ if and only if $\mathbf{R}$ has full rank in $\mathbb{Z}_p$. Hence, we can deduce from the previous case that the number of Hankel matrices of full rank equals $(p-1)p^{(\alpha-1)(2d-1)+(2d-2)}$. If we choose $b \leftarrow U(\mathbb{Z}_q^{<n+d-1}[x])$, then

$$\Pr\left[\operatorname{rank}(\mathbf{Hank}(b)) = d\right] = \frac{(p-1)p^{(\alpha-1)(2d-1)+(2d-2)}}{p^{\alpha(2d-1)}} = 1 - \frac{1}{p}.$$

For $d < n$, using the same argument as before, the probability is at least $1 - \frac{1}{p}$.

Case 3 *($q = \prod_{i \in [l]} p_i^{\alpha_i}$).* For the case $d = n$, it follows from the Chinese remainder theorem that the number of Hankel matrices of full rank d modulo q equals the product of the number of Hankel matrices of full rank d modulo $p_i^{\alpha_i}$ which is given by

$$\prod_{i \in [l]} (p_i - 1) p_i^{(\alpha_i - 1)(2d-1)+(2d-2)}.$$

Thus, if we choose $b \leftarrow U(\mathbb{Z}_q^{<n+d-1}[x])$, then

$$\Pr\left[\operatorname{rank}(\mathbf{Hank}(b)) = d\right] = \prod_{i \in [l]} \left(1 - \frac{1}{p_i}\right).$$

Similarly as before, for $d < n$ and $b \leftarrow U(\mathbb{Z}_q^{<n+d-1}[x])$, then

$$\Pr\left[\operatorname{rank}(\mathbf{Hank}(b)) = d\right] \geq \prod_{i \in [l]} \left(1 - \frac{1}{p_i}\right).$$

□

We denote by $(\mathbb{Z}_q^{<n+d-1}[x])^\times$ the set of polynomials of $\mathbb{Z}_q^{<n+d-1}[x]$ with Hankel matrix of full rank d. Note that for $a \in \mathbb{Z}_q^{<n}[x]$ and $b \in \mathbb{Z}_q^{<n+d-1}[x]$, the middle-product can be represented as a matrix-vector product

$$a \odot_d b = \mathbf{Hank}(b) \cdot \overline{a}.$$

Lemma 10. *Let d and n be two integers with $0 < d \leq n$ and b a fixed element of $\left(\mathbb{Z}_q^{<n+d-1}[x]\right)^\times$. If we choose $a \leftarrow U(\mathbb{Z}_q^{<n}[x])$, then $a \odot_d b$ is uniformly random in $\mathbb{Z}_q^{<d}[x]$.*

Proof. We can write $a \odot_d b = \mathbf{Hank}(b) \cdot \overline{a}$. For any $d \leq n$ and full rank matrix $\mathbf{A} \in \mathbb{Z}_q^{d \times n}$, the mapping from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q^d$ given by multiplication with $\mathbf{A}$ is surjective. As a is chosen uniformly at random and the Hankel matrix of b has full rank d, the middle-product is also uniformly distributed. □

4 Middle-Product Learning With Rounding

In this section, we define in the first subsection the new assumption and then show in the second subsection its hardness by reducing the MP-LWE problem to it.

4.1 Definition of the MP-CLWR assumption

In the following, we define the *Middle-Product Computational Learning With Rounding* (MP-CLWR) assumption which is an adaption of the *Ring Computational Learning With Rounding* (R-CLWR) assumption from Chen et al. [CZZ18] to the middle-product setting. For a detailed introduction and motivation of this computational notion, see [CZZ18, Section 3].

In order to define this computational assumption, we need to introduce our experiment setting. Within the experiment, three different parties in form of algorithms appear: A challenger $\mathcal{C}$ interacting with an adversary $\mathcal{A}$ who is receiving its samples from a source $\mathcal{S}$. All three algorithms are restricted to be probabilistic and polynomial-time (PPT). As a first step, the source $\mathcal{S}$ generates a sample (X, aux) using two sets called var and con. It then sends this sample to the challenger $\mathcal{C}$, which computes, with the help of this sample, a tuple $(\mathsf{Input}, \mathsf{Target})$. The adversary only receives the Input part of the tuple to compute Output. The adversary wins the experiment if Output equals Target.

```
$\mathsf{Exp}(\mathcal{C}, \mathcal{A}, \mathcal{S})$
$(X, \mathsf{aux}) \leftarrow \mathcal{S}(\mathsf{var}, \mathsf{con})$
$(\mathsf{Input}, \mathsf{Target}) \leftarrow \mathcal{C}(X, \mathsf{aux})$
$(\mathsf{Output}) \leftarrow \mathcal{A}(\mathsf{Input})$
return $\mathsf{Output} = \mathsf{Target}$
```

Fig. 1. The experiment $\mathsf{Exp}(\mathcal{C}, \mathcal{A}, \mathcal{S})$.

The idea of the computational assumption is to consider two different experiments with the same challenger $\mathcal{C}$ and adversary $\mathcal{A}$ but with different sources $\mathcal{S}_1$ and $\mathcal{S}_2$, which differ in the distribution var but have the same distribution con, motivating the notation var for variable and con for constant. The new notion guarantees that if $\mathcal{A}$ cannot compute Target from X_1 generated by $\mathcal{S}_1$, then it is not able to compute Target from X_2 generated by $\mathcal{S}_2$ either.

We illustrate the new notion in Figure 2 below. Let $\mathcal{C}$ be an arbitrary challenger. If the success probability of any adversary $\mathcal{A}$ outputting the correct answer in $\mathsf{Exp}_1(\mathcal{C}, \mathcal{A}, \mathcal{S}_1)$ is negligible, then it is in $\mathsf{Exp}_2(\mathcal{C}, \mathcal{A}, \mathcal{S}_2)$ as well.

```
$\mathsf{Exp}_1(\mathcal{C}, \mathcal{A}, \mathcal{S}_1)$
$(X_1, \mathsf{aux}) \leftarrow \mathcal{S}_1(\mathsf{var}_1, \mathsf{con})$
$(\mathsf{Input}_1, \mathsf{Target}_1) \leftarrow \mathcal{C}(X_1, \mathsf{aux})$
$\mathsf{Output}_1 \leftarrow \mathcal{A}(\mathsf{Input}_1)$
return $\mathsf{Output}_1 = \mathsf{Target}_1$
```

```
$\mathsf{Exp}_2(\mathcal{C}, \mathcal{A}, \mathcal{S}_2)$
$(X_2, \mathsf{aux}) \leftarrow \mathcal{S}_2(\mathsf{var}_2, \mathsf{con})$
$(\mathsf{Input}_2, \mathsf{Target}_2) \leftarrow \mathcal{C}(X_2, \mathsf{aux})$
$\mathsf{Output}_2 \leftarrow \mathcal{A}(\mathsf{Input}_2)$
return $\mathsf{Output}_2 = \mathsf{Target}_2$
```

Fig. 2. Experiment setting of the computational assumption.

Now, we define our new MP-CLWR assumption which is an adaption of the R-CLWR assumption from [CZZ18] to the middle-product setting. As an analog of the notion of units in the original paper, we define $(\mathbb{Z}_q^{<n+d-1}[x])^\times$ as the set of all polynomials over $\mathbb{Z}_q$ having degree less than $n+d-1$ and a Hankel matrix of order $d \times n$ of full rank d. The integers d and n define the parameters of the middle-product, q defines the general and p the rounding modulus. The number of samples has to be fixed beforehand and is given by t.

Definition 6 (MP-CLWR assumption) *Let d, n, p, q and t be positive integers fulfilling $0 < d \leq n$ and $q \geq p \geq 2$. Choose s uniformly at random over $(\mathbb{Z}_q^{<n+d-1}[x])^\times$. Denote by $\mathcal{X}_s$ the distribution of $(a, \lfloor a \odot_d s \rceil_p)$, where $a \leftarrow U(\mathbb{Z}_q^{<n}[x])$, and denote by $\mathcal{U}$ the distribution of $(a, \lfloor b \rceil_p)$, where $a \leftarrow U(\mathbb{Z}_q^{<n}[x])$ and $b \leftarrow U(\mathbb{Z}_q^{<d}[x])$. For $i \in \{1, 2\}$ define the input for $\mathcal{S}_i$ as $(\mathsf{var}_i, \mathsf{con})$, where var_1 denotes the distribution $\mathcal{X}_s^t$, and var_2 the distribution $\mathcal{U}^t$, and con is an arbitrary distribution over $\{0,1\}^*$ which is independent from var_1 and var_2. For a fixed challenger $\mathcal{C}$ let $\mathcal{P}_{\mathcal{C},\mathcal{A}}$ be the probability for an adversary $\mathcal{A}$ to win $\mathsf{Exp}_1(\mathcal{C}, \mathcal{A}, \mathcal{S}_1)$, while $\mathcal{Q}_{\mathcal{C},\mathcal{A}}$ be that for $\mathcal{A}$ to win $\mathsf{Exp}_2(\mathcal{C}, \mathcal{A}, \mathcal{S}_2)$.*

The MP-CLWR$_{p,q,n,d,t}$ *assumption states that for any challenger $\mathcal{C}$ if $\mathcal{Q}_{\mathcal{C},\mathcal{A}}$ is negligible for any adversary $\mathcal{A}$, so is $\mathcal{P}_{\mathcal{C},\mathcal{A}}$. We call the difference $|\mathcal{P}_{\mathcal{C},\mathcal{A}} - \mathcal{Q}_{\mathcal{C},\mathcal{A}}|$ the advantage of the adversary $\mathcal{A}$.*

Correspondingly, we also define the *Middle-Product Computational Rounded Learning With Errors* (MP-CRLWE) assumption which is important in the hardness reduction in Section 4.2 below.

Definition 7 (MP-CRLWE assumption) *Let d, n, p, q and t be positive integers fulfilling $0 < d \leq n$ and $q \geq p \geq 2$. Choose s uniformly at random over $(\mathbb{Z}_q^{<n+d-1}[x])^\times$. Let χ_e be the error distribution over $\mathbb{R}^{<d}[x]$. Denote by $\mathcal{Y}_{s,\chi_e}$ the distribution of $(a, \lfloor a \odot_d s + e \rceil_p)$, where $a \leftarrow U(\mathbb{Z}_q^{<n}[x])$ and $e \leftarrow \chi_e$ and denote by $\mathcal{U}$ the distribution of $(a, \lfloor b \rceil_p)$ where $a \leftarrow U(\mathbb{Z}_q^{<n}[x])$ and $b \leftarrow U(\mathbb{Z}_q^{<d}[x])$. For $i \in \{1, 2\}$ define the input for $\mathcal{S}_i$ as $(\mathsf{var}_i, \mathsf{con})$, where var_1 denotes the distribution $\mathcal{Y}_{s,\chi_e}^t$, and var_2 the distribution $\mathcal{U}^t$, and con is an arbitrary distribution over $\{0,1\}^*$ which is independent from var_1 and var_2. For a fixed challenger $\mathcal{C}$ let $\mathcal{P}'_{\mathcal{C},\mathcal{A}}(\chi_e)$ be the probability for an adversary $\mathcal{A}$ to win $\mathsf{Exp}_1(\mathcal{C}, \mathcal{A}, \mathcal{S}_1)$, while $\mathcal{Q}_{\mathcal{C},\mathcal{A}}$ be that for $\mathcal{A}$ to win $\mathsf{Exp}_2(\mathcal{C}, \mathcal{A}, \mathcal{S}_2)$.*

The MP-CRLWE$_{p,q,n,d,t,\chi_e}$ *assumption related to the error distribution χ_e states that for any challenger $\mathcal{C}$ if $\mathcal{Q}_{\mathcal{C},\mathcal{A}}$ is negligible for any adversary $\mathcal{A}$, so is $\mathcal{P}'_{\mathcal{C},\mathcal{A}}(\chi_e)$. We call the difference $\left|\mathcal{P}'_{\mathcal{C},\mathcal{A}}(\chi_e) - \mathcal{Q}_{\mathcal{C},\mathcal{A}}\right|$ the advantage of the adversary $\mathcal{A}$.*

4.2 Hardness of MP-CLWR

We now prove the hardness of MP-CLWR with the help of a reduction from the decisional MP-LWE problem to the MP-CLWR problem. The decisional version of MP-LWE itself can be reduced from the decisional P-LWE problem for a large class of defining polynomials, see Theorem 1. As P-LWE benefits from worst-case to average-case reductions from lattice problems, our new MP-CLWR assumption also enjoys the worst-case hardness.

Theorem 2 (Hardness of MP-CLWR). *Let d, n, p, q and t be positive integers with $0 < d \leq n$ and $q \geq p \geq 2$. Further, let $q = \prod_{i \in [l]} p_i^{\alpha_i}$ be the prime power factorization of q with some $l > 0$, where p_i is prime and $\alpha_i > 0$ for all $i \in [l]$. Let χ be an error distribution over $\mathbb{R}^{<d}[x]$ which is balanced and B-bounded with probability at least δ, fulfilling $q > 2pBdt$ and $\delta \geq 1 - \frac{1}{td}$. There is a reduction from the decisional $\text{MP-LWE}_{q,n,d,\chi}$ problem to the $\text{MP-CLWR}_{p,q,n,d,t}$ problem, with t the number of samples fixed beforehand.*

Assume that the advantage of an MP-CLWR solver is ε. Then, there is an MP-LWE solver with advantage at least

$$\left(\frac{1}{e^2} \left(\varepsilon + \mathcal{Q}_{\mathcal{C},\mathcal{A}} \right)^2 \right) \cdot \prod_{i \in [l]} \left(1 - \frac{1}{p_i} \right).$$

In order to prove the theorem, we show the following sequence of reductions:

$$\begin{tikzcd}
\text{MP-LWE}_{q,n,d,\chi} \arrow[r, "\text{Lemma 11}"] \arrow[d, dashed] & \text{MP-LWE}^{\times}_{q,n,d,\chi} \arrow[d, "\text{Lemma 12}"] \\
\text{MP-CLWR}_{p,q,n,d,t} & \text{MP-CRLWE}_{p,q,n,d,t,\chi} \arrow[l, "\text{Lemma 13}"]
\end{tikzcd}$$

The first reduction is achieved by a standard technique.

Lemma 11. *Let d, n, p, q and t be positive integers, such that it yields $0 < d \leq n$ and $q \geq p \geq 2$. Let χ_e be the error distribution over $\mathbb{R}^{<d}[x]$. Further, let the unique prime power factorization of q be given by $q = \prod_{i \in [l]} p_i^{\alpha_i}$ with some $l > 0$, where p_i is prime and $\alpha_i > 0$ for all $i \in [l]$. If there is a PPT algorithm solving $\text{MP-LWE}^{\times}_{q,n,d,\chi}$ with non-negligible advantage ε, then there is a PPT algorithm solving $\text{MP-LWE}_{q,n,d,\chi}$ with non-negligible advantage at least*

$$\varepsilon \cdot \prod_{i \in [l]} \left(1 - \frac{1}{p_i} \right).$$

Proof. Let $(a_i, b_i)_{i \in [t]}$ be the given input tuple of samples of $\text{MP-LWE}_{q,n,d,\chi}$, where $s \leftarrow U(\mathbb{Z}_q^{n+d-1}[x])$. An adversary can take this tuple of samples $(a_i, b_i)_i$ and query an oracle of $\text{MP-LWE}^{\times}_{q,n,d,\chi}$ on it. As showed in Lemma 9, the probability that the Hankel matrix of s has full rank d is at least $\prod_{i \in [l]} \left(1 - \frac{1}{p_i} \right)$. Assuming that the oracle succeeds with non-negligible probability ε in general, it will now succeed with probability at least $\varepsilon \cdot \prod_{i \in [l]} \left(1 - \frac{1}{p_i} \right)$, which completes the proof. □

The following lemma is an adaption of Lemma 12 in [CZZ18] into our context.

Lemma 12 (MP-LWE to MP-CRLWE). *Assume that the advantage of any PPT algorithm to solve the decisional* $\mathrm{MP\text{-}LWE}^{\times}_{q,n,d,\chi}$ *problem is less than* ε*, then we have*

$$\left|\mathcal{P}'_{\mathcal{C},\mathcal{A}}(\chi) - \mathcal{Q}_{\mathcal{C},\mathcal{A}}\right| < \varepsilon,$$

for any PPT adversary $\mathcal{A}$ *and PPT challenger* $\mathcal{C}$*. Thus, there is a reduction from* $\mathrm{MP\text{-}LWE}^{\times}_{q,n,d,\chi}$ *to* $\mathrm{MP\text{-}CRLWE}_{p,q,n,d,t,\chi}$*, with* t *the number of samples fixed beforehand.*

Proof. In order to show this reduction, we will construct an adversary $\mathcal{B}$ to solve the decisional $\mathrm{MP\text{-}LWE}_{q,n,d,\chi}$ problem. This adversary $\mathcal{B}$ will at the same time play the role of the challenger $\mathcal{C}$ in the MP-CRLWE experiment. At the beginning, $\mathcal{B}$ receives a tuple of samples $(x_i, y_i)_{i\in[t]}$. It sets $a_i = x_i$ and $b_i = \lfloor y_i \rceil_p$ for all $i \in [t]$ and $X = (a_i, b_i)_{i\in[t]}$. As a challenger of the experiment, $\mathcal{B}$ can compute the corresponding Input and Target. $\mathcal{B}$ also verifies if the Output of $\mathcal{A}$ equals the Target. If this is the case, $\mathcal{B}$ outputs 1, otherwise 0.

If $(x_i, y_i)_i$ are MP-LWE samples, then are $(a_i, b_i)_i$ samples from $\mathcal{Y}_{s,\chi}$, used in the MP-CRLWE assumption. Thus, $\Pr(\mathcal{B}((x_i, y_i)_i) = 1) = \mathcal{P}'_{\mathcal{C},\mathcal{A}}(\chi)$. On the other hand, if $(x_i, y_i)_i$ is a tuple of uniform samples, then is $(a_i, b_i)_i$ also uniformly distributed. Hence, $\Pr(\mathcal{B}((x_i, y_i)_i) = 1) = \mathcal{Q}_{\mathcal{C},\mathcal{A}}$. Assuming the hardness of decisional MP-LWE, we have $\left|\mathcal{P}'_{\mathcal{C},\mathcal{A}}(\chi) - \mathcal{Q}_{\mathcal{C},\mathcal{A}}\right| < \varepsilon$, for negligible ε and for any adversary $\mathcal{A}$. In particular, the MP-CRLWE assumption holds: If $\mathcal{Q}_{\mathcal{C},\mathcal{A}}$ is negligible, so is $\mathcal{P}'_{\mathcal{C},\mathcal{A}}$ for the same challenger $\mathcal{C}$ and adversary $\mathcal{A}$ using the equation above. □

The following reduction is an adaption of Lemma 8 and Lemma 9 in [CZZ18], based on the results of [BGM+16], together with our results about random Hankel matrices of Section 3.

Lemma 13 (MP-CRLWE to MP-CLWR). *Let* $s \in (\mathbb{Z}_q^{<n+d-1}[x])^{\times}$*. Let* $\mathcal{X}_s$ *and* $\mathcal{Y}_s$ *denote the random variables of a single* MP-CLWR *sample* $(a, \lfloor a \odot_d s \rceil_p)$ *and a single* MP-CRLWE $(a, \lfloor a \odot_d s + e \rceil_p)$ *sample, respectively. Further, let* χ *be an error distribution which is balanced and* B*-bounded with probability at least* δ *over* $\mathbb{Z}_q^{<d}[x]$*, where* $q > 2pBdt$ *and* $\delta \geq 1 - \frac{1}{td}$*. Then we have*

$$(\mathcal{P}_{\mathcal{C},\mathcal{A}})^2 \leq \mathcal{P}'_{\mathcal{C},\mathcal{A}}(\chi) \cdot e^2,$$

where e *is the Euler's number.*

Hence, there is a reduction from $\mathrm{MP\text{-}CRLWE}_{p,q,n,d,t,\chi}$ *to* $\mathrm{MP\text{-}CLWR}_{p,q,n,d,t}$*.*

Proof. Using Lemma 6 about the multiplicativity and the probability preservation property from the Rényi divergence, we have

$$(\mathcal{P}_{\mathcal{C},\mathcal{A}})^2 \leq \mathcal{P}'_{\mathcal{C},\mathcal{A}}(\chi) \cdot \mathrm{RD}_2(\mathcal{X}_s \| \mathcal{Y}_s)^t.$$

In the following we show that the Rényi divergence of $\mathcal{X}_s$ and $\mathcal{Y}_s$ fulfills

$$\mathrm{RD}_2(\mathcal{X}_s \| \mathcal{Y}_s) \leq \frac{(1 + 2pB/q)^d}{\delta^d}.$$

Following the definition of the Rényi divergence it yields

$$\begin{aligned}\mathrm{RD}_2(\mathcal{X}_s\|\mathcal{Y}_s) &= E_{a\leftarrow U(\mathbb{Z}_q^{<n}[x])}\frac{\Pr\left[\mathcal{X}_s=(a,\lfloor a\odot_d s\rceil_p)\right]}{\Pr\left[\mathcal{Y}_s=(a,\lfloor a\odot_d s\rceil_p)\right]}\\ &= E_{a\leftarrow U(\mathbb{Z}_q^{<n}[x])}\frac{1}{\Pr_{e\leftarrow\chi}\left[\lfloor a\odot_d s+e\rceil_p=\lfloor a\odot_d s\rceil_p\right]}.\end{aligned}$$

First, we define the border elements in $\mathbb{Z}_q$ with regard to B and p by

$$Bor_{p,q}(B)=\left\{x\in\mathbb{Z}_q\colon\ \lfloor x+B\rceil_p\neq\lfloor x\rceil_p\right\}.$$

These are the elements in $\mathbb{Z}_q$ which are close to the rounding boundary. It yields $|Bor_{p,q}(B)|\leq 2Bp$. For $0\leq t\leq d$, let us also define

$$Bad_{s,t}=\left\{a\in\mathbb{Z}_q^{<n}[x]\colon\ |\{i\in[d]\colon(a\odot_d s)_i\in Bor_{p,q}(B)\}|=t\right\}.$$

In other words, $Bad_{s,t}$ defines, for a given polynomial s and number of coefficients t, the set of polynomials a in $\mathbb{Z}_q^{<n}[x]$ such that the middle-product $a\odot_d s$ has exactly t coefficients close to the rounding boundary. Now we fix t and assume $a\in Bad_{s,t}$. For any $i\in[d]$ with $(a\odot_d s)_i\notin Bor_{p,q}(B)$, it yields

$$\Pr_{e_i}\left[\lfloor(a\odot_d s)_i+e_i\rceil_p=\lfloor(a\odot_d s)_i\rceil_p\right]\geq\delta,$$

as e_i is sampled from the distribution χ which is B-bounded with probability at least δ. If $(a\odot_d s)_i\in Bor_{p,q}(B)$, then

$$\Pr_{e_i}\left[\lfloor(a\odot_d s)_i+e_i\rceil_p=\lfloor(a\odot_d s)_i\rceil_p\right]\geq\frac{1}{2},$$

because e_i is sampled from a balanced distribution. Thus, the probabilities of $e_i\in[-B,0]$ or in $[0,B]$ are each greater or equal to $\frac{1}{2}$ and $\lfloor(a\odot_d s)_i+e_i\rceil_p\neq\lfloor(a\odot_d s)_i\rceil_p$ happens in exactly one of the two cases. Since each coefficient of e is independently distributed and $a\odot_d s$ has exactly t coefficients in $Bor_{p,q}(B)$, it yields

$$\Pr_{e\leftarrow\chi}\left[\lfloor a\odot_d s+e\rceil_p=\lfloor a\odot_d s\rceil_p\right]\geq\frac{1}{2^t}\cdot\delta^{d-t}\geq\frac{1}{2^t}\cdot\delta^d.$$

By Lemma 10, we know that if a is uniform in $\mathbb{Z}_q^{<n}[x]$, so is $a\odot_d s\in\mathbb{Z}_q^{<d}[x]$. Thus, it yields

$$\Pr\left[a\in Bad_{s,t}\right]\leq\binom{d}{t}\left(1-\frac{|Bor_{p,q}(B)|}{q}\right)^{d-t}\left(\frac{|Bor_{p,q}(B)|}{q}\right)^{t}.$$

Hence,

$$\begin{aligned}\mathrm{RD}_2(\mathcal{X}_s \| \mathcal{Y}_s) &\leq \delta^{-d} \sum_{t\in[d]} 2^t \cdot \Pr\left[a \in Bad_{s,t}\right] \\ &= \delta^{-d} \sum_{t\in[d]} \binom{d}{t} \left(1 - \frac{|Bor_{p,q}(B)|}{q}\right)^{d-t} \left(2 \cdot \frac{|Bor_{p,q}(B)|}{q}\right)^{t} \\ &= \delta^{-d} \left(1 + \frac{|Bor_{p,q}(B)|}{q}\right)^{d} \\ &\leq \delta^{-d} \left(1 + \frac{2pB}{q}\right)^{d}.\end{aligned}$$

From the results above, we can derive

$$\mathrm{RD}_2(\mathcal{X}_s \| \mathcal{Y}_s)^t \leq \frac{(1+2pB/q)^{td}}{\delta^{td}} \leq \frac{(1+1/td)^{td}}{(1-1/td)^{td}} \approx e^2,$$

where $\delta \geq 1 - \frac{1}{td}$ and $q > 2pBdt$. □

5 A Public Key Encryption Scheme Based on MP-CLWR

In this section, we present a Public Key Encryption (PKE) scheme whose security is based on the hardness of the middle-product computational learning with rounding problem (MP-CLWR, see Section 4.1). Its design is inspired by the PKE scheme from Roşca et al. [RSSS17] based on the hardness of the middle-product learning with errors (MP-LWE, see Section 2.4) problem and by the PKE scheme from Chen et al. [CZZ18] based on the hardness of the ring computational learning with rounding problem. As a first step, we define the scheme and show its correctness in Section 5.1. Subsequently, we prove its security based on the hardness of MP-CLWR in Section 5.2.

5.1 Definition and Correctness

In this section, we define the PKE scheme and show its correctness under a proper choice of parameters. We use the reconciliation rounding function $\lfloor \cdot \rceil_2 : \mathbb{Z}_q \to \mathbb{Z}_2$, the reconciliation cross-rounding function $\langle \cdot \rangle_2 : \mathbb{Z}_q \to \mathbb{Z}_2$, the randomized doubling function $\mathtt{DBL}\colon \mathbb{Z}_q \to \mathbb{Z}_{2q}$ and the reconciliation algorithm $\mathtt{REC}$ from Section 2.2. As we only need the randomized doubling function $\mathtt{DBL}$ for q odd, we set it to be the identity function for q even.

Recall that $\mathtt{INV}(\cdot)$ denotes the probabilistic lifting function from $\mathbb{Z}_p[x]$ to $\mathbb{Z}_q[x]$ for two integers p and q with $2 \leq p \leq q$. We need $\mathtt{INV}(\cdot)$ to lift rounded polynomials in $\mathbb{Z}_p[x]$ to $\mathbb{Z}_q[x]$ such that $\left\lfloor \mathtt{INV}(\lfloor a \rceil_p) \right\rceil_p = \lfloor a \rceil_p$. Note that $\mathtt{INV}(\lfloor a \rceil_p) = a + e$ with $\|e\|_\infty \leq \frac{q}{p}$.

Let H denote a random oracle $H\colon \{0,1\}^d \to \{0,1\}^k$. Further, let k, d, n, p, q and t be positive integers with $d + k \leq n$ and $q \geq p \geq 2$. The plaintext space is $\{0,1\}^{<k}[x]$.

1. $\mathsf{KGen}(1^\lambda)$. Sample $s \leftarrow U\left((\mathbb{Z}_q^{<n+d+k-1}[x])^\times\right)$ such that $\mathbf{Hank}(s)$ has full rank[5]. For $i \in [t]$, choose $a_i \leftarrow U(\mathbb{Z}_q^{<n}[x])$ and compute $b_i = \lfloor a_i \odot_{d+k} s \rceil_p$. Return $\mathsf{pk} = (a_i, b_i)_{i\in[t]}$ and $\mathsf{sk} = s$.
2. $\mathsf{Enc}(\mathsf{pk}, \mu)$. For $i \in [t]$, sample $r_i \leftarrow U(\{0,1\}^{<k+1}[x])$ and set the first part of the ciphertext as
$$c_1 = \sum_{i\in[t]} r_i a_i \bmod q.$$
Compute $v = \sum_{i\in[t]} r_i \odot_d \mathtt{INV}(b_i) \bmod q$. Set the second and third part of the ciphertext as
$$c_2 = \langle \mathtt{DBL}(v)\rangle_2 \text{ and } c_3 = H(\lfloor \mathtt{DBL}(v)\rceil_2) \oplus \mu.$$
Return $c = (c_1, c_2, c_3)$.
3. $\mathsf{Dec}(\mathsf{sk}, c)$. Compute $w = c_1 \odot_d s$ and return $\mu' = c_3 \oplus H(\mathtt{REC}(w, c_2))$.

Lemma 14 (Correctness). *Assume that $p > 8t(k+1)$. For every plaintext μ and key pair $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(1^\lambda)$, we have*
$$\Pr(\mathsf{Dec}(\mathsf{sk}, \mathsf{Enc}(\mathsf{pk}, \mu)) = \mu) = 1.$$

Proof. In order to prove the correctness of the scheme, we need to guarantee that the reconciliation mechanism succeeds. Following Lemma 4 we have to show that $\|w - v\|_\infty < q/8$. Notice that we have
$$v = \sum_{i\in[t]} r_i \odot_d \mathtt{INV}(b_i) = \sum_{i\in[t]} r_i \odot_d (a_i \odot_{d+k} s + e_i) = \sum_{i\in[t]} (r_i a_i) \odot_d s + \sum_{i\in[t]} r_i \odot_d e_i$$
$$= c_1 \odot_d s + \sum_{i\in[t]} r_i \odot_d e_i = w + \sum_{i\in[t]} r_i \odot_d e_i,$$
where $\|e_i\|_\infty < q/p$ for $i \in [t]$ is determined by the lifting function $\mathtt{INV}(\cdot)$. Thus it suffices to have
$$\left\|\sum_{i\in[t]} r_i \odot_d e_i\right\|_\infty < q/8.$$
For $i \in [t]$ each coefficient of $r_i \odot_d e_i$ can be seen as the inner product $\langle u, v\rangle$ of a binary vector u of dimension $k+1$ and a vector v also of dimension $k+1$, where each coefficient has magnitude $\leq q/p$. Notice that we have
$$|\langle u, v\rangle| \leq \|u\|_2 \cdot \|v\|_2 \leq \sqrt{k+1} \cdot \sqrt{(k+1)\cdot q^2/p^2} = (k+1)q/p.$$
Hence, it yields
$$\left\|\sum_{i\in[t]} r_i \odot_d e_i\right\|_\infty \leq \sum_{i\in[t]} \|r_i \odot_d e_i\|_\infty \leq t(k+1)q/p.$$
As $p > 8t(k+1)$, we have $t(k+1)q/p < q/8$ which guarantees that the reconciliation mechanism succeeds. □

[5] This can be done by sampling $s \leftarrow U\left(\mathbb{Z}_q^{<n+d+k-1}[x]\right)$ uniformly at random and rejecting it if its Hankel matrix is not full rank.

5.2 Provable Security

In this section, we prove the security of the PKE scheme defined above based on the hardness of MP-CLWR.

Lemma 15 (Security). *Let λ be the security parameter. Further, let k, d, n, p, q and t be positive integers such that it yields $d + k \leq n$ and $q \geq p \geq 2$. Assume that $t \geq (2 \cdot \lambda + (k + d + n) \cdot \log q)/(k + 1)$. The PKE scheme above is* $\mathsf{IND\text{-}CPA}$ *secure in the Random Oracle Model under the* $\text{MP-CLWR}_{p,q,n,d+k,t}$ *hardness assumption.*

Proof. The $\mathsf{IND\text{-}CPA}$ security game is the following: A challenger $\mathcal{C}$ generates a key pair $(\mathsf{pk}, \mathsf{sk})$, samples a random bit b and sends the public key pk to the adversary $\mathcal{A}$. The adversary chooses two messages m_0, m_1 and sends them to the challenger $\mathcal{C}$, which in turn encrypts m_b and sends the corresponding ciphertext c back to $\mathcal{A}$. The adversary outputs a bit b' as a guess of b and wins the game if $b = b'$. The game is illustrated in Figure 3.

```
$\text{IND-CPA}^{\mathcal{A}}_{\mathsf{Enc}}$
$b \xleftarrow{\$} \{0,1\}$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(1^\lambda)$
$(m_0, m_1) \leftarrow \mathcal{A}(1^\lambda, \mathsf{pk})$
$c \leftarrow \mathsf{Enc}(\mathsf{pk}, m_b)$
$b' \leftarrow \mathcal{A}(1^\lambda, \mathsf{pk}, c)$
return $b = b'$
```

Fig. 3. The $\mathsf{IND\text{-}CPA}$ security game.

If the Random Oracle H was not queried on the value of $\lfloor \mathtt{DBL}(v) \rceil_2 \in \{0,1\}^d$ during the game, the adversary $\mathcal{A}$ can only guess the (randomly chosen) bit b with success probability 1/2. In particular, we can use a successful adversary $\mathcal{A}$ of the $\mathsf{IND\text{-}CPA}$ security game to construct a successful adversary $\mathcal{A}'$ which outputs $\lfloor \mathtt{DBL}(v) \rceil_2$, given the first two parts (c_1, c_2) of any ciphertext $c = (c_1, c_2, c_3)$. These first two parts are independent of the message to encrypt. We will call this the $\mathsf{COMP\text{-}DBL}$ game.

During the $\mathsf{IND\text{-}CPA}$ game, $\mathcal{A}'$ answers the random oracle queries of $\mathcal{A}$ by maintaining an input-output table for H. For each query, $\mathcal{A}'$ first checks if H was already programmed on the queried input. If yes, it outputs the corresponding hash value, otherwise it chooses a fresh random value and sets H accordingly. Assuming $\mathcal{A}$ has non-negligible advantage to win the $\mathsf{IND\text{-}CPA}$ security game, it must have queried H on $\lfloor \mathtt{DBL}(v) \rceil_2$, hence $\mathcal{A}'$ can look up the pair $(\lfloor \mathtt{DBL}(v) \rceil_2, r)$ with $r = H(\lfloor \mathtt{DBL}(v) \rceil_2)$ in the random oracle table. The procedure is illustrated in Figure 4 below.

As a next step, we need to show that the probability of $\mathcal{A}'$ to win is negligible under the MP-CLWR assumption. We will consider the following sequence of

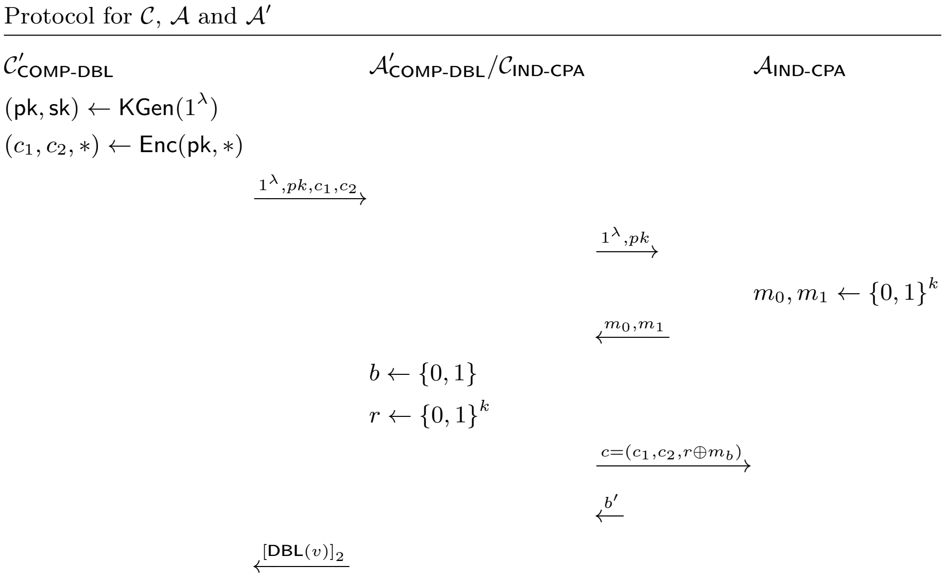
Protocol for $\mathcal{C}$, $\mathcal{A}$ and $\mathcal{A}'$
$\mathcal{C}'_{\mathsf{COMP\text{-}DBL}}$
$\mathcal{A}'_{\mathsf{COMP\text{-}DBL}}/\mathcal{C}_{\mathsf{IND\text{-}CPA}}$
$\mathcal{A}_{\mathsf{IND\text{-}CPA}}$
$(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(1^\lambda)$
$(c_1, c_2, *) \leftarrow \mathsf{Enc}(\mathsf{pk}, *)$
$\xrightarrow{1^\lambda, pk, c_1, c_2}$
$\xrightarrow{1^\lambda, pk}$
$m_0, m_1 \leftarrow \{0,1\}^k$
$\xleftarrow{m_0, m_1}$
$b \leftarrow \{0,1\}$
$r \leftarrow \{0,1\}^k$
$\xrightarrow{c=(c_1, c_2, r \oplus m_b)}$
$\xleftarrow{b'}$
$\xleftarrow{\lceil \mathtt{DBL}(v) \rfloor_2}$

Fig. 4. Using $\mathcal{A}$ of the $\mathsf{IND\text{-}CPA}$ security game to win the $\mathsf{COMP\text{-}DBL}$ game.

games, where in all games $a_i \leftarrow U(\mathbb{Z}_q^{<n}[x])$ for $i \in [t]$ and the secret s is chosen via $s \leftarrow U\left((\mathbb{Z}_q^{<n+d+k-1}[x])^\times\right)$. Further, we sample $r_i \leftarrow U(\{0,1\}^{<k+1}[x])$ for $i \in [t]$ and set the first part of the ciphertext as $c_1 = \sum_{i \in [t]} r_i a_i \bmod q$.

The adversary $\mathcal{A}'$ receives in each game the tuple $(1^\lambda, \mathsf{pk}, c_1, c_2)$ and its target is to compute $\lfloor \mathtt{DBL}(v) \rceil_2$, where v is specified by each game separately. Game 1 corresponds to the $\mathsf{COMP\text{-}DBL}$ game above.

G1 : Set $b_i = \lfloor a_i \odot_{d+k} s \rceil_p$, $\mathsf{pk} = (a_i, b_i)_i$, $v = \sum_i \mathtt{INV}(b_i) \odot_d r_i \bmod q$, and $c_2 = \langle \mathtt{DBL}(v) \rangle_2$,

G2 : Set $b_i \leftarrow \left\lfloor U(\mathbb{Z}_q^{<d+k}[x]) \right\rceil_p$, $\mathsf{pk} = (a_i, b_i)_i$, $v = \sum_i \mathtt{INV}(b_i) \odot_d r_i \bmod q$, and $c_2 = \langle \mathtt{DBL}(v) \rangle_2$,

G3 : Set $b_i \leftarrow \left\lfloor U(\mathbb{Z}_q^{<d+k}[x]) \right\rceil_p$, $\mathsf{pk} = (a_i, b_i)_i$, $v \leftarrow U(\mathbb{Z}_q^{<d}[x])$, and $c_2 = \langle \mathtt{DBL}(v) \rangle_2$.

Note that in the last game, c_1 and c_2 are independent and hence the probability that $\mathcal{A}'$ outputs $\lfloor \mathtt{DBL}(v) \rceil_2 \in \{0,1\}^d$ is exactly $1/2^d$, using Lemma 3.

Furthermore, the second and third game are within exponentially small statistical distance, using the generalized leftover hash lemma. In more detail, the statistical distance of the two distributions of $((a_i, b_i)_i, c_1, v)$ in Game 2 and 3 is given by

$$\Delta \left[\left((a_i, b_i)_i, \sum_{i \in [t]} r_i a_i, \sum_{i \in [t]} r_i \odot_d \mathtt{INV}(b_i) \right), \left((a_i, b_i)_i, \sum_{i \in [t]} r_i a_i, v \right) \right] \leq 2^{-\lambda},$$

where for all $i \in [t]$ the polynomials a_i, b_i, r_i and v are chosen uniformly at random in $\mathbb{Z}_q^{<n}[x]$, $\lfloor \mathbb{Z}_q^{<d+k}[x] \rceil_p$, $\{0,1\}^{<k+1}[x]$ and $\mathbb{Z}_q^{<d}[x]$, respectively. Note that the randomness of $(h_{(b_i)_i})_{(b_i)_i}$ comes from the randomness of $(b_i)_i$ and since Lemma 8 shows that $(h_{(b_i)_i})_{(b_i)_i}$ is universal we can use Lemma 5. Thus, the statistical distance is bounded above by

$$\frac{1}{2} \cdot \sqrt{2^{-(k+1)t} \cdot q^{k+n+d}}.$$

Recall the data processing inequality of the statistical distance

$$\Delta(P^f, Q^f) \leq \Delta(P, Q)$$

for any function f, where P^f (resp. Q^f) denotes the distribution of $f(y)$ induced by sampling $y \leftarrow P$ (resp. $y \leftarrow Q$). Setting $f = \langle \mathtt{DBL}(\cdot) \rangle$, we get

$$\Delta\left(((a_i, b_i)_i, c_1, c_2), ((a_i, b_i)_i, c_1, u)\right) \leq 2^{-\lambda}.$$

The first and second game differ only in the way how the b_i are computed. In the first game, b_i is a rounded middle-product sample and in the latter one, it is a rounded uniform sample. We can interpret this situation as two different experiments, see Figure 5.

```
$\mathsf{Exp}_1(\mathcal{C}, \mathcal{A}, \mathcal{S}_1)$
$((a_i, \lfloor a_i \odot_d s \rceil_p)_i, \mathsf{aux}) \leftarrow (\mathcal{X}_s^t, \mathsf{con})$
$(\mathsf{Input}_1, \lfloor \mathtt{DBL}(v) \rceil_2) \leftarrow \mathcal{C}((a_i, b_i)_i, \mathsf{aux})$
$\mathsf{Output}_1 \leftarrow \mathcal{A}(\mathsf{Input}_1)$
return $\mathsf{Output}_1 = \lfloor \mathtt{DBL}(v) \rceil_2$
```

```
$\mathsf{Exp}_2(\mathcal{C}, \mathcal{A}, \mathcal{S}_2)$
$((a_i, b_i)_i, \mathsf{aux}) \leftarrow (\mathcal{U}^t, \mathsf{con})$
$(\mathsf{Input}_2, \lfloor \mathtt{DBL}(v) \rceil_2) \leftarrow \mathcal{C}((a_i, b_i)_i, \mathsf{aux})$
$\mathsf{Output}_2 \leftarrow \mathcal{A}(\mathsf{Input}_2)$
return $\mathsf{Output}_2 = \lfloor \mathtt{DBL}(v) \rceil_2$
```

Fig. 5. Experiment setting of the security proof.

Recall from Definition 6 that $\mathcal{X}_s^t$ denotes the distribution of $(a_i, \lfloor a_i \odot_d s \rceil_p)_i$, where we choose the $a_i \leftarrow U(\mathbb{Z}_q^{<n}[x])$ independently and sample a fixed secret element $s \leftarrow U\left((\mathbb{Z}_q^{<n+d+k-1}[x])^{\times}\right)$. Further, we denote by $\mathcal{U}^t$ the distribution of $(a_i, \lfloor b_i \rceil_p)_i$, where we choose the $a_i \leftarrow U(\mathbb{Z}_q^{<n}[x])$ and the $b_i \leftarrow U(\mathbb{Z}_q^{<d+k}[x])$ independently. In addition, con is an arbitrary distribution over $\{0,1\}^*$ which is independent from $\mathcal{X}_s^t$ and $\mathcal{U}^t$. The Input_1 of the first experiment $\mathsf{Exp}_1(\mathcal{C}, \mathcal{A}, \mathcal{S}_1)$ is given by $(1^\lambda, \mathsf{pk}, c_1, \langle \mathtt{DBL}(v) \rangle_2)$, where $v = \sum_i \mathtt{INV}(b_i) \odot_d r_i$ with $b_i = \lfloor a_i \odot_{d+k} s \rceil_p$. On the other hand, the Input_2 of the second experiment $\mathsf{Exp}_2(\mathcal{C}, \mathcal{A}, \mathcal{S}_2)$ is defined by $(1^\lambda, \mathsf{pk}, c_1, \langle \mathtt{DBL}(v) \rangle_2)$, where we still have $v = \sum_i \mathtt{INV}(b_i) \odot_d r_i$ but this time with $b_i \leftarrow \lfloor U(\mathbb{Z}_q^{<d+k}[x]) \rceil_p$. The Target is in both cases the same, namely $\lfloor \mathtt{DBL}(v) \rceil_2$.

According to the MP-CLWR assumption, if the success probability for any $\mathcal{A}$ to output the requested $\lfloor \mathtt{DBL}(v) \rceil_2$ is negligible when $b_i \leftarrow \lfloor U(\mathbb{Z}_q^{<d+k}[x]) \rceil_p$, it is also negligible when b_i is an MP-LWR instance.

Combining the arguments above shows that the success probability of $\mathcal{A}'$ is negligible under the MP-CLWR assumption, completing the security proof of our PKE scheme. □

6 Parameters and Comparison

6.1 Asymptotic Parameters

As example parameters we set the dimension $n \geq \lambda$, $k = d = n/2$, $t = \Theta(\log(n))$, $q = \Theta(n^{4+c}\log(n)^2)$ and $p = \Theta(n\log(n))$, where c is an arbitrary positive constant and λ the underlying security parameter. Using these parameters, the scheme is correct (Lemma 14) and secure under the MP-CLWR$_{p,q,n,d+k,t}$ assumption (Lemma 15). This allows us to rely on the MP-LWE$_{q,n,d+k,\chi}$ problem (Theorem 2), where the error distribution χ is B-bounded with $B = O(n^{2+c})$. Using the P-LWE$^f_{q,D_{\beta q}}$ to MP-LWE$_{q,n,d+k,D_{\alpha q}}$ reduction (Theorem 1), this in turn prevents attack as [AG11], where $\beta = \Omega(\sqrt{n}/q)$ for any f monic of degree n with constant coefficient coprime with q and expansion factor at least n^c.

We now compare our encryption scheme with the one of [RSSS17]. Figure 6 shows the asymptotic parameters, key sizes and ciphertext sizes for both schemes. The most important parameter is the value $\log(q)$ as it dominates the key and ciphertext sizes of both schemes. Asymptotically, in both cases this value is $\Theta(\log(n))$.

Parameter	[RSSS17]	Our work
n	$\geq \lambda$	$\geq \lambda$
c	> 0	> 0
k	$n/2$	$n/2$
d	$n/2$	$n/2$
t	$\Theta(\log(n))$	$\Theta(\log(n))$
q	$\Theta(n^{2.5+c}\sqrt{\log(n)})$	$\Theta(n^{4+c}\log(n)^2)$
$\log(q)$	$\Theta(\log(n))$	$\Theta(\log(n))$
α	$\Theta\left(\frac{1}{n\sqrt{\log(n)}}\right)$	-
p	-	$\Theta(n\log(n))$
B	-	$O(n^{2+c})$
Key size		
sk	$(n+d+k-1)\cdot\log(q)$	$(n+d+k-1)\cdot\log(q)$
pk	$t\cdot((n+d+k)\log(q))$	$t\cdot(n\log(q)+(d+k)\log(p))$
Ciphertext size		
c_1	$(n+k)\log(q)$	$(n+k)\log(q)$
c_2	$d\log(q)$	d
c_3	-	k

Fig. 6. Comparison of asymptotic parameters, key sizes and ciphertext sizes

In general, the sampling cost is one of the intense operations of an encryption scheme. In the encryption scheme of [RSSS17], we need $2\cdot t+1$ sampling subroutines, including t from a rounded Gaussian distribution, during key generation and t sampling subroutines during encryption. In contrast, in our case we only need $t+1$ sampling subroutine during key generation and t sampling subroutines during encryption. Additionally, in our case all sampling is performed over some uniform distribution which is more efficient than Gaussian type sampling.

Further, in our encryption scheme we don't need to restrict the modulus q to be prime. Unlike [RSSS17], it works for all integer moduli which are sufficiently large. This gives an advantage on the choice of parameters.

6.2 Concrete Security

Unfortunately, Theorem 2 gives no guidance on the choice of parameters nor on their concrete security. Parameter derivation is indeed an active research topic for lattice based cryptography, for both the construction of cryptographic protocols and cryptanalysis, e.g., [CN11,Pei16,ACD+18]. In practice, it is common to derive the parameters by looking at the cost of the best known attacks, such as BKZ with quantum sieving, e.g., [ADPS16,AKS01]. Below, we present the best known attacks against our scheme. This analysis follows the literature by treating rounded polynomials by p as polynomials mod q with small noises, see for instance [APS15].

6.2.1 Attack on public keys Two common approaches to analyze LWE problems are primal attacks (also known as decoding attacks) and dual attacks (also known as distinguish attacks), e.g. [APS15].

Primal attack. The middle-product of two polynomials can be expressed as the product of some (slightly differently defined) Toeplitz matrix associated to one of the polynomials by the reversed coefficient vector of the second polynomial [RSSS17, Lemma 3.2]. In order to avoid confusion with the Toeplitz matrix **Toep** we defined in Section 3, we will denote the matrix simply by $\mathbf{T}$. For any positive integers d and k, and a polynomial $a \in \mathbb{Z}_q^{<k}[x]$, we let $\mathbf{T}^{d,k}(a)$ denote the matrix in $\mathbb{Z}_q^{d\times(k+d-1)}$ whose i-th row is given by the coefficients of $x^{i-1} \cdot a$, for $i \in [d]$. Thus, given a public key $\mathsf{pk} = (a_i, b_i)_{i\in[t]}$ with $a_i \in \mathbb{Z}_q^{<n}[x]$ and $b_i = \lfloor a_i \odot_{d+k} s \rceil_p$, where $s \in \mathbb{Z}_q^{<n+d+k-1}[x]$, it yields

$$\bar{\mathbf{b}_i} = \left\lfloor \mathbf{T}^{d+k,n}(a_i) \cdot \bar{\mathbf{s}} \right\rceil_p .$$

Transposing and multiplying it by q/p gives

$$q/p \cdot \bar{\mathbf{b}}_i^T = \bar{\mathbf{s}}^T \cdot \left(\mathbf{T}^{d+k,n}(a_i)\right)^T + \mathbf{e}_i^T,$$

for some $\mathbf{e}_i$ with $\|\mathbf{e}_i\|_\infty < q/2p$. Note that in Section 2.2, we point out hat the coefficients of the noise $\mathbf{e}_i$ lie between 0 and q/p. So it is best for the attacker to treat them as elements from $-q/2p$ to $q/2p$. This gives a smaller bound and is hence easier to attack. Therefore, one is able to build a lattice spanned by the row vector of the following matrix $\mathbf{A}_1$ defined by

$$\mathbf{A}_1 = \begin{pmatrix} q\mathbf{I}_{d+k} & \dots & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \dots & q\mathbf{I}_{d+k} & 0 & 0 \\ \left(\mathbf{T}^{d+k,n}(a_1)\right)^T & \dots & \left(\mathbf{T}^{d+k,n}(a_{t_0})\right)^T & \mathbf{I}_{d+k+n-1} & 0 \\ q/p \cdot \bar{\mathbf{b}}_1^T & \dots & q/p \cdot \bar{\mathbf{b}}_{t_0}^T & 0 & 1 \end{pmatrix},$$

for some $t_0 \leq t$ (the attacker can choose arbitrary, up to t, number of a_i's to attack). Here, $\mathbf{I}_n$ denotes the identity matrix of order $n \times n$. For appropriate parameters, the attacker may be able to recover a vector $\mathbf{v} = (\mathbf{e}_1, \dots, \mathbf{e}_{t_0}, -\bar{\mathbf{s}}, 1)^T$ for some $\|\mathbf{e}_1, \dots, \mathbf{e}_{t_0}\|_\infty < q/2p$, if this vector is sufficiently shorter than Gaussian Heuristic. This lattice has a dimension of $\dim = (d+k)t_0 + n + d + k$, and a determinant $q^{(d+k)t_0}$. On the other hand,

$$\|\mathbf{v}\|_2 \leq \sqrt{(d+k)t_0(q/2p)^2 + (n+d+k-1)(q/2)^2 + 1}.$$

As per [GN08], the hardness of recovering such a vector is determined by the dim-th root of the quantity

$$\begin{aligned} \gamma_1 &= \sqrt{\frac{\dim}{2\pi e}} \frac{\det(\mathbf{A}_1)^{\frac{1}{\dim}}}{\|\mathbf{v}\|_2} \\ &= \sqrt{\frac{(d+k)t_0 + n + d + k}{2\pi e}} \frac{q^{\frac{(d+k)t_0}{(d+k)t_0+n+d+k}}}{\sqrt{(d+k)t_0(q/2p)^2 + (n+d+k-1)(q/2)^2 + 1}}. \end{aligned}$$

We need $\gamma_1^{\frac{1}{\dim}} \leq 1.0045$ for all $t_0 \in [t]$ to achieve 128 bits of security against BKZ attacks [CN11] under the quantum-Core-sieve model [ADPS16].

Dual attack. An attacker can use the dual attack to distinguish the middle-product LWR samples from uniform. Given the public keys $(a_i, b_i)_{i \in [t]}$, the attacker first converts the polynomial b_i from a polynomial in $\mathbb{Z}_p^{<d+k}[x]$ to $\mathbb{Z}_q^{<d+k}[x]$ like before. So each b_i can be represented as $q/p \cdot b_i = a_i \odot_{d+k} s + e_i$ with $\|e_i\|_\infty \leq q/2p$. Now consider the (scaled) dual lattice

$$\Lambda_q(a_1, a_2, \dots, a_t) = \left\{ (x_1, x_2, \dots, x_t) \in \left(\mathbb{Z}^{<d+k}\right)^t : \sum_i x_i \cdot a_i = 0 \mod q \right\}.$$

If the adversary is able to find a short lattice vector in $\Lambda_q(a_1, a_2, \dots, a_t)$, then $\sum_i x_i \odot_d b_i$ is small if b_i-s are MP-LWR samples; it is large and uniform if b_i-s are uniform. This is because when $b_i = a_i \odot_{d+k} s + e_i$, then $\sum_i x_i \odot_d b_i = \sum_i x_i \odot_d (a_i \odot_{d+k} s + e_i) = \sum_i (x_i \cdot a_i) \odot_d s + x_i \odot_d e_i = \sum_i x_i \odot_d e_i$. And for proper parameters, $\sum_i x_i \odot_d e_i$ will be small. Thus, this dual attack allows one to solve decisional MP-LWR problems.

The attack works when the ratio between the error and the modulus is not much bigger that $1/\|x_1, x_2, \ldots, x_n\|_\infty$ [MR09]. For our concrete parameters, we will be aiming for the error to be 1.5 times bigger than $1/\|x_1, x_2, \ldots, x_n\|_\infty$. Thus from the results of [MR09], we have

$$\frac{q/2p}{q} \lessapprox 1.5 \cdot \frac{1}{\|x_1, x_2, \ldots, x_n\|_\infty},$$

that is, if one can find a short vector in $\Lambda_q(a_1, a_2, \ldots, a_t)$ with infinity norm less than $3p$, then one will be able to build such a distinguisher.

To recover a short vector from lattice $\Lambda_q(a_1, a_2, \ldots, a_t)$ in practice, one may run lattice reduction algorithms over a lattice spanned by the row vector of the following matrix $\mathbf{A}_2$ defined by

$$\mathbf{A}_2 = \begin{pmatrix} q\mathbf{I}_{n+k} & 0 & 0 & \ldots & 0 \\ \mathbf{T}^{k+1,n}(a_1) & \mathbf{I}_{k+1} & 0 & \ldots & 0 \\ \mathbf{T}^{k+1,n}(a_2) & 0 & \mathbf{I}_{k+1} & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{T}^{k+1,n}(a_t) & 0 & 0 & \ldots & \mathbf{I}_{k+1} \end{pmatrix},$$

where $\mathrm{dim} = (n+k) + t(k+1)$ and the determinant is q^{n+k}. The vector $\mathbf{x} = (0, x_1, x_2, \ldots, x_n)$ will be a (short) vector in the lattice. The l_2 norm is bounded by $\sqrt{t(k+1)}\frac{3p}{2}$, since each x_i is bounded by $3p$. Applying same analysis we had in the previous section, we have a Hermite factor

$$\begin{aligned} \gamma_2 &= \sqrt{\frac{\mathrm{dim}}{2\pi e}} \frac{\|\mathbf{x}\|_2}{\det(\mathbf{A}_2)^{\frac{1}{\mathrm{dim}}}} \\ &= \sqrt{\frac{n+(t+1)k+t}{2\pi e}} \frac{\sqrt{t(k+1)}\frac{3p}{2}}{q^{\frac{n+k}{n+(t+1)k+t}}}. \end{aligned}$$

The attacker may recover $\mathbf{x}$ (and solve the decisional problem) if $\gamma_2 > 1.0045^{\mathrm{dim}}$.

6.2.2 Attack on the ciphertext Given a ciphertext $c = (c_1, c_2, c_3)$, enciphered under the polynomials a_i of the public key, we have

$$c_1 = \sum_{i \in [t]} r_i a_i \bmod q,$$

where the polynomials $(r_i)_{i \in [t]}$ are sampled uniformly from $\{0,1\}^{<k+1}[x]$. Recall, that the matrix $\mathbf{T}$ also helps to formulate the product of two polynomials as a matrix-vector-product. More concretely, $r_i \cdot a_i$ can be written as $\mathbf{r}_i^T \cdot \mathbf{T}^{k+1,n}(a_i)$. It is crucial that the polynomials $(r_i)_{i \in [t]}$ are hidden from the attacker. The attacker may therefore be able to build a lattice spanned by the row vectors of the following basis:

$$\mathbf{A}_3 = \begin{pmatrix} \mathbf{A}_2 & 0 \\ c_1 & 1 \end{pmatrix},$$

that contains the vector $\mathbf{v} = (0, \mathbf{r}_1, \ldots, \mathbf{r}_t, -1)^T$. The dimension of the lattice is $n + k + t(k+1) + 1 = n + (t+1)(k+1)$. The determinant of the lattice is q^{n+k} since the degree of c_1 is $n + k$. The norm of the target vector is $\sqrt{(k+1)t/2}$, since all r_i's are binary polynomials. Therefore, we require that

$$\gamma_3 = \sqrt{\frac{n+(t+1)(k+1)}{2\pi e}} \frac{q^{\frac{n+k}{n+(t+1)(k+1)}}}{\sqrt{(k+1)t/2}} \leq 1.0045^{n+(t+1)(k+1)}.$$

6.2.3 Concrete parameters We summarize our parameters in Fig. 7. Those parameters are robust against the three attacks that we have shown in the previous section. We note that the proposed parameter set may not be optimal. As the middle product problems are relative new, and we do not currently know any attacks that outperform attacks against classical LWE problems, we take a conservative route by deriving parameters from an adaption of the parameters proposed by [RSSS17]. This leaves adequate security margins even if middle product problems turn out to be a lot easier. We leave optimal and more efficient instantiations, and dedicated cryptanalysis to future work.

Parameter	[RSSS17]	Our work
n	512	512
c	0.01	0.01
k	256	256
d	256	256
t	9	9
q	18.941.623	18.941.623
$\log(q)$	25	25
α	0.000651	-
p	-	18.504
B	-	279.019
Key size		
sk	25.575	25.575
pk	230.400	184.320
Ciphertext size		
c_1	19.200	19.200
c_2	6.400	256
c_3	-	256
$c = (c_1, c_2, c_3)$	25.600	19.712

Fig. 7. Comparison of example parameters, key sizes and ciphertext sizes for $c = 0.01$ and $n = 512$.

Acknowledgments

This work is supported by the European Union PROMETHEUS project (Horizon 2020 Research and Innovation Program, grant 780701). This work has also received a French government support managed by the National Research Agency in the ”Investing for the Future” program, under the national project RISQ P141580-2660001 / DOS0044216, and under the project TYREX granted by the CominLabs excellence laboratory with reference ANR-10-LABX-07-01. This work is also supported through NATO SPS Project G5448 and through NIST awards 60NANB18D216 and 60NANB18D217.

Katharina Boudgoust is funded by the Direction Générale de l'Armement (Pôle de Recherche CYBER). Dipayan Das is funded by MHRD, India.

We also thank our anonymous referees for their helpful and constructive feedback.

References

AA16. J. Alperin-Sheriff and D. Apon. Dimension-preserving reductions from LWE to LWR. *IACR Cryptology ePrint Archive*, 2016:589, 2016.

ACD$^+$18. M. R. Albrecht, B. R. Curtis, A. Deo, A. Davidson, R. Player, E. W. Postlethwaite, F. Virdia, and T. Wunderer. Estimate all the {LWE, NTRU} schemes! In *Security and Cryptography for Networks - 11th International Conference, SCN 2018, Amalfi, Italy, September 5-7, 2018, Proceedings*, pages 351–367, 2018.

ADPS16. E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe. Post-quantum key exchange - A new hope. In *25th USENIX Security Symposium, USENIX Security 16, Austin, TX, USA, August 10-12, 2016.*, pages 327–343, 2016.

AG11. S. Arora and R. Ge. New algorithms for learning in presence of errors. In *Automata, Languages and Programming - 38th International Colloquium, ICALP 2011, Zurich, Switzerland, July 4-8, 2011, Proceedings, Part I*, pages 403–415, 2011.

AKPW13. J. Alwen, S. Krenn, K. Pietrzak, and D. Wichs. Learning with rounding, revisited - new reduction, properties and applications. In *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I*, pages 57–74, 2013.

AKS01. M. Ajtai, R. Kumar, and D. Sivakumar. A sieve algorithm for the shortest lattice vector problem. In *Proceedings on 33rd Annual ACM Symposium on Theory of Computing, July 6-8, 2001, Heraklion, Crete, Greece*, pages 601–610, 2001.

APS15. M. R. Albrecht, R. Player, and S. Scott. On the concrete hardness of learning with errors. *J. Mathematical Cryptology*, 9(3):169–203, 2015.

BBF$^+$19. H. Baan, S. Bhattacharya, S. R. Fluhrer, Ó. García-Morchón, T. Laarhoven, R. Rietman, M.-J. O. Saarinen, L. Tolhuizen, and Z. Zhang. Round5: Compact and fast post-quantum public-key encryption. In *Post-Quantum Cryptography - 10th International Conference, PQCrypto 2019, Chongqing, China, May 8-10, 2019 Revised Selected Papers*, pages 83–102, 2019.

BDJ06. W. Bryc, A. Dembo, and T. Jiang. Spectral measure of large random Hankel, Markov and Toeplitz matrices. *Ann. Probab.*, 34(1):1–38, 2006.

BGM$^+$16. A. Bogdanov, S. Guo, D. Masny, S. Richelson, and A. Rosen. On the hardness of learning with rounding over small modulus. In *Theory of Cryptography - 13th International Conference, TCC 2016-A, Tel Aviv, Israel, January 10-13, 2016, Proceedings, Part I*, pages 209–224, 2016.

BHLY16. L. Groot Bruinderink, A. Hülsing, T. Lange, and Y. Yarom. Flush, gauss, and reload - A cache attack on the BLISS lattice-based signature scheme. In *Cryptographic Hardware and Embedded Systems - CHES 2016 - 18th International Conference, Santa Barbara, CA, USA, August 17-19, 2016, Proceedings*, pages 323–345, 2016.

BLL$^+$15. S. Bai, A. Langlois, T. Lepoint, D. Stehlé, and R. Steinfeld. Improved security proofs in lattice-based cryptography: Using the rényi divergence rather than the statistical distance. In *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part I*, pages 3–24, 2015.

BLP$^+$13. Z. Brakerski, A. Langlois, C. Peikert, O. Regev, and D. Stehlé. Classical hardness of learning with errors. In *Symposium on Theory of Computing Conference, STOC'13, Palo Alto, CA, USA, June 1-4, 2013*, pages 575–584, 2013.

BPR11. A. Banerjee, C. Peikert, and A. Rosen. Pseudorandom functions and lattices. *IACR Cryptology ePrint Archive*, 2011:401, 2011.

BPR12. A. Banerjee, C. Peikert, and A. Rosen. Pseudorandom functions and lattices. In *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, pages 719–737, 2012.

CIV16. W. Castryck, I. Iliashenko, and F. Vercauteren. Provably weak instances of ring-lwe revisited. In *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part I*, pages 147–167, 2016.

CN11. Y. Chen and P. Q. Nguyen. BKZ 2.0: Better lattice security estimates. In *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, pages 1–20, 2011.

CZZ18. L. Chen, Z. Zhang, and Z. Zhang. On the hardness of the computational ring-lwr problem and its applications. In *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part I*, pages 435–464, 2018.

DB15. C. Du and G. Bai. Towards efficient discrete gaussian sampling for lattice-based cryptography. In *25th International Conference on Field Programmable Logic and Applications, FPL 2015, London, United Kingdom, September 2-4, 2015*, pages 1–6, 2015.

DKRV18. J.-P. D'Anvers, A. Karmakar, S. Sinha Roy, and F. Vercauteren. Saber: Module-lwr based key exchange, cpa-secure encryption and cca-secure KEM. In *Progress in Cryptology - AFRICACRYPT 2018 - 10th International Conference on Cryptology in Africa, Marrakesh, Morocco, May 7-9, 2018, Proceedings*, pages 282–305, 2018.

DXL12. J. Ding, X. Xie, and X. Lin. A simple provably secure key exchange scheme based on the learning with errors problem. *IACR Cryptology ePrint Archive*, 2012:688, 2012.

GN08. N. Gama and P. Q. Nguyen. Predicting lattice reduction. In *Advances in Cryptology - EUROCRYPT 2008, 27th Annual International Conference on* *the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008. Proceedings*, pages 31–51, 2008.

KL96. E. Kaltofen and A. Lobo. On rank properties of toeplitz matrices over finite fields. In *ISSAC*, volume 96, pages 241–249, 1996.

LM06. V. Lyubashevsky and D. Micciancio. Generalized compact knapsacks are collision resistant. In *Automata, Languages and Programming, 33rd International Colloquium, ICALP 2006, Venice, Italy, July 10-14, 2006, Proceedings, Part II*, pages 144–155, 2006.

LPR10. V. Lyubashevsky, C. Peikert, and O. Regev. On ideal lattices and learning with errors over rings. In *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Monaco / French Riviera, May 30 - June 3, 2010. Proceedings*, pages 1–23, 2010.

LS15. A. Langlois and D. Stehlé. Worst-case to average-case reductions for module lattices. *Des. Codes Cryptogr.*, 75(3):565–599, 2015.

Lyu16. V. Lyubashevsky. Digital signatures based on the hardness of ideal lattice problems in all rings. In *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part II*, pages 196–214, 2016.

MR09. D. Micciancio and O. Regev. Lattice-based cryptography. In *Post-Quantum Cryptography, D. J. Bernstein, J. Buchmann, E. Dahmen (Eds)*, pages 147–191. Springer, 2009.

NIS. NIST. Post-quantum cryptography standardization. `https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization`.

Pei09. C. Peikert. Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009, Bethesda, MD, USA, May 31 - June 2, 2009*, pages 333–342, 2009.

Pei14. C. Peikert. Lattice cryptography for the internet. In *Post-Quantum Cryptography - 6th International Workshop, PQCrypto 2014, Waterloo, ON, Canada, October 1-3, 2014. Proceedings*, pages 197–219, 2014.

Pei16. C. Peikert. How (not) to instantiate ring-lwe. In *Security and Cryptography for Networks - 10th International Conference, SCN 2016, Amalfi, Italy, August 31 - September 2, 2016, Proceedings*, pages 411–430, 2016.

Pes16. P. Pessl. Analyzing the shuffling side-channel countermeasure for lattice-based signatures. In *Progress in Cryptology - INDOCRYPT 2016 - 17th International Conference on Cryptology in India, Kolkata, India, December 11-14, 2016, Proceedings*, pages 153–170, 2016.

R6́1. Alfréd Rényi. On measures of entropy and information. In *Proc. 4th Berkeley Sympos. Math. Statist. and Prob., Vol. I*, pages 547–561. Univ. California Press, Berkeley, Calif., 1961.

Reg05. O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005*, pages 84–93, 2005.

Reg09. O. Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6):34:1–34:40, 2009.

RSSS17. M. Rosca, A. Sakzad, D. Stehlé, and R. Steinfeld. Middle-product learning with errors. In *Advances in Cryptology - CRYPTO 2017 - 37th Annual*

International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part III, pages 283–297, 2017.

RSW18. M. Roşca, D. Stehlé, and A. Wallet. On the ring-lwe and polynomial-lwe problems. In *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part I*, pages 146–173, 2018.

Saa18. M.-J. O. Saarinen. Arithmetic coding and blinding countermeasures for lattice signatures - engineering a side-channel resistant post-quantum signature scheme with compact signatures. *J. Cryptographic Engineering*, 8(1):71–84, 2018.

SSTX09. D. Stehlé, R. Steinfeld, K. Tanaka, and K. Xagawa. Efficient public key encryption based on ideal lattices. In *Advances in Cryptology - ASIACRYPT 2009, 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, December 6-10, 2009. Proceedings*, pages 617–635, 2009.

vEH14. T. van Erven and P. Harremoës. Rényi divergence and kullback-leibler divergence. *IEEE Trans. Information Theory*, 60(7):3797–3820, 2014.