Non-norm Elements for Cryptography: Extended Abstract

Andrew Mendelsohn and Cong Ling

Department of EEE, Imperial College London, London, SW7 2AZ, United Kingdom.
andrew.mendelsohn18@imperial.ac.uk, c.ling@imperial.ac.uk

Introduction In [8], noncommutative division algebras were used to create space-time block codes (STBCs) satisfying 'nice' properties, such as having rate at least 1 and being full rank. The family of algebras used were *cyclic division algebras*, constructed as follows:

Let L/K be a finite Galois extension of number fields. Suppose the Galois group of L/K is cyclic, so $\mathrm{Gal(L/K)} = \langle\theta\rangle$ for some automorphism θ. Let $\gamma \in K$. We then define an algebra $\mathcal{A}$:

$$\mathcal{A} := L \oplus uL \oplus ... \oplus u^{d-1}L,$$

where u is an auxiliary element satisfying $u^d = \gamma$ and $ux = \theta(x)u$, for all $x \in L$. This is called a cyclic algebra, denoted $\mathcal{A} = (L/K, \theta, \gamma)$. $\mathcal{A}$ is a *division* algebra if every non-zero element has a multiplicative inverse.

The development of CDA-based codes was continued in [3] and [10], among others. All these works required $\mathcal{A}$ to be division. A necessary and sufficient condition for $\mathcal{A}$ to be a cyclic division algebra (CDA) is given below, which reduces the creation of CDAs to finding non-norm elements:

Proposition 1. *[1] The cyclic algebra $\mathcal{A}$ is a division algebra if and only if γ satisfies the non-norm condition.*

An element $x \in K$ is *non-norm* if $\nexists\ y \in L$: $N_{L/K}(y) = x$. One says x *satisfies the non-norm condition* if every power x^i, $0 < i < [L : K]$, is non-norm.

This led to researchers developing techniques to construct non-norm elements. One such work developed a construction of non-norm elements to create CDAs which yield so-called *perfect* codes [6]. To achieve this, they require non-norm elements γ of unit-magnitude, that is $|\gamma| = 1$, which are fractional, i.e. $\gamma \in K \setminus \mathcal{O}_K$. They take $K \in \{\mathbb{Q}(i), \mathbb{Q}(\zeta_3)\}$ to be a cyclotomic field of degree two.

Extending [6] for PIDs In our work, we extend the methods of [6]. We first observe that the authors' result on non-norm elements can be straightforwardly extended to hold for large classes of field extensions:

Theorem 1. *Let L/K be a degree n cyclic Galois extension and $\mathcal{O}_K$ a PID. If q is a prime that splits into precisely two ideals in $\mathcal{O}_K$ which are inert in $\mathcal{O}_L$, then the ratio of the generators of the ideals is a non-norm element for L/K.*

Proof. The proof follows [6, Proposition 2/3] mutatis mutandis. □

As a consequence, we apply this to cyclotomic fields:

Corollary 1. *Let $K = \mathbb{Q}(\zeta_m)$ and define the sets*

$$S := \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 25, 27, 33, 35, 45\},$$

and

$$S' = \{4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 60, 84\}.$$

If $m \in S \cup S'$ or $m \in 2S$, then if L/K is a degree n cyclic Galois extension and q splits into precisely two ideals in $\mathcal{O}_K$ which are inert in $\mathcal{O}_L$, then the ratio of the generators of the ideals is a non-norm element for L/K.

Proof. The specified m precisely yield $\mathbb{Q}(\zeta_m)$ with PID ring of integers. □

One can obtain unit-magnitude non-norm elements from the above theorem if q splits into two ideals in K not fixed by complex conjugation. This can be extended to hold for greater splitting. For an example, take $K = \mathbb{Q}(\zeta_{32})$ and $L = \mathbb{Q}(\zeta_7 + \zeta_7^{-1}, \zeta_{64})$. L is a compositum of $\mathbb{Q}(\zeta_{64})$ and $\mathbb{Q}(\zeta_7 + \zeta_7^{-1}, \zeta_{32})$, which are cyclic over K of coprime degrees, so L/K is cyclic of degree 6. Set $q = 773$; q is unramified in L, and $q \equiv 5 \bmod 32$, which has order 8, so $f^q_{K|\mathbb{Q}} = 8$. We then find $g^q_{K|\mathbb{Q}} = [K : \mathbb{Q}]/f^q_{K|\mathbb{Q}} = 2$, so q splits into two primes in K, $\mathfrak{p}_1$ and $\mathfrak{p}_2$.

$\mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/7\mathbb{Z})^\times/\{\pm 1\} \times (\mathbb{Z}/64\mathbb{Z})^\times$ so $f^q_{L|\mathbb{Q}}$ is the smallest f such that $q^f \equiv \pm 1 \bmod 448$. Observe that $q \equiv 325 \bmod 448$, which has order 48. Furthermore, $q^{24} \not\equiv -1 \bmod 448$ so $f^q_{L|\mathbb{Q}} = 48$. Since $[L : K] = 96$, we obtain $g^q_{L|\mathbb{Q}} = [L : \mathbb{Q}]/f^q_{L|\mathbb{Q}} = 96/48 = 2$. This then implies $g^q_{L|K} = 1$, so $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are inert in L. Since $\mathbb{Z}[\zeta_{32}]$ is a PID, we can then take the ratio of the generators of $\mathfrak{p}_1$ and $\mathfrak{p}_2$ for a unit-magnitude non-norm element γ, and construct a CDA $\mathcal{A} = (L/K, \theta, \gamma)$, where $[\mathcal{A} : \mathbb{Q}] = 6^2 \cdot 16 = 576$.

Extending [5] to non-PIDs We then show that one can construct fractional unit-magnitude non-norm elements for L/K with $\mathcal{O}_K$ not a PID. We use

Lemma 1. *[9] Let L/K be a degree n Galois extension and $\mathfrak{q}$ be a prime ideal in K below the prime ideal $\mathfrak{Q}$ in L. Let $f = f_{\mathfrak{Q}|\mathfrak{q}}$ be the relative inertial degree of $\mathfrak{Q}$ over $\mathfrak{q}$. If $\gamma \in \mathfrak{q} \setminus \mathfrak{q}^2$, then $\gamma^i \notin N_{L/K}(L^\times)$ for $i = 1, 2, ..., f-1$.*

And then prove a number of new results:

Lemma 2. *Let L/K be a degree n Galois extension and $\mathfrak{p}$ be a prime ideal in K below the prime ideal $\mathfrak{P}$ in L. Let $f = f_{\mathfrak{P}|\mathfrak{p}}$ be the relative inertial degree of $\mathfrak{P}$ over $\mathfrak{p}$. Suppose $\gamma \in \mathcal{O}_K \setminus \mathcal{O}_K^\times$ is such that $\gamma^i \notin N_{L/K}(L^\times)$ for $i = 1, 2, ..., f-1$. Then there exists a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ such that γ is contained in $\mathfrak{p} \setminus \mathfrak{p}^2$.*

Proposition 2. *Let L/K be Galois of degree n. Suppose we have two non-norm elements in $\mathcal{O}_K$, γ_1 and γ_2. Assume γ_i lies in an ideal as in Lemma 1, so $\gamma_i \in \mathfrak{q}_i \setminus \mathfrak{q}_i^2$, for $\mathfrak{q}_i$ a prime ideal of $\mathcal{O}_K$, lying above some fixed prime $q \in \mathbb{Z}$, for $i = 1, 2$. If $\gamma_2 \notin \mathfrak{q}_1$, then $\gamma_1\gamma_2^j$ is a non-norm element, for powers $j < f^q_{L|K}$.*

Corollary 2. *Suppose γ_1 and γ_2 are non-unit non-norm elements of L/K such that $\gamma_1\gamma_2$ is also non-norm. Then $\gamma_1\gamma_2^{-1}$ is a non-unit non-norm element.*

And use a known property of cyclotomic fields:

Lemma 3. *Let $K = \mathbb{Q}(\zeta_n)$ and $p \in \mathbb{Z}$ be an unramified prime. Write $g^p_{K|\mathbb{Q}} = g$ and $\Phi_n(x) \equiv f_1(x)f_2(x)...f_g(x) \bmod p$, with $\Phi_n(x)$ the nth cyclotomic polynomial and the $f_i(x)$ monic irreducible. Let $\mathfrak{p}_i$ be a prime ideal containing $f_i(\zeta_n)$. Then for any $i \in \{1, 2, ..., g\}$, there exists a choice of $f_i(x)$ such that $f_i(\zeta_n) \notin \mathfrak{p}_i^2$.*

Finally, we prove our main result:

Theorem 2. *Let K be a cyclotomic field, and L/K a degree n Galois extension. If q is an unramified prime such that*

1. *q splits into at least two ideals in $\mathcal{O}_K$ which are inert in $\mathcal{O}_L$, and*
2. *the prime ideals above q in $\mathcal{O}_K$ are permuted by complex conjugation,*

then the ratio of a non-integer generator of any of the $\mathcal{O}_K$-ideals with its complex conjugate is a non-norm element for L/K.

Proof. We consider q splitting into two ideals in $\mathcal{O}_K$; greater splitting is proved similarly. Write $q\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, where $\mathfrak{p}_i = (q, f_i(\zeta_n))$, $i = 1, 2$. By Lemma 3, choose $f_1(x)$ such that $f_1(\zeta_n) \notin \mathfrak{p}_1^2$. By Lemma 1, since $\mathfrak{p}_1$ is inert in L by assumption, $f_1(\zeta_n)$ is a non-norm element for L/K. Consider $\overline{f_1(\zeta_n)}$; since the prime ideals above q are permuted by complex conjugation, we have $\overline{f_1(\zeta_n)} \notin \mathfrak{p}_1$, so $\overline{f_1(\zeta_n)} \in \mathfrak{p}_2$. If $\overline{f_1(\zeta_n)} \in \mathfrak{p}_2^2$, then $f_1(\zeta_n) \in \overline{\mathfrak{p}_2^2} = \overline{\mathfrak{p}_2}^2 = \mathfrak{p}_1^2$, a contradiction. So $\overline{f_1(\zeta_n)} \in \mathfrak{p}_2 \setminus \mathfrak{p}_2^2$ and hence is a non-norm element. By Proposition 2, $f_1(\zeta_n)\overline{f_1(\zeta_n)}$ is non-norm, and by Corollary 2, $f_1(\zeta_n)\overline{f_1(\zeta_n)}^{-1}$ is non-norm. □

For example, let $K = \mathbb{Q}(\zeta_{190})$ and $L = \mathbb{Q}(\zeta_{190}, \zeta_{11} + \zeta_{11}^{-1})$. Note $[L : K] = 5$ and $[K : \mathbb{Q}] = 72$. Set $q = 41$. Then $f^q_{K|\mathbb{Q}} = 18$ and $f^q_{L|\mathbb{Q}} = 90$, so $f^q_{L|K} = 5$, $g^q_{L|K} = [L : K]/f^q_{L|K} = 1$, and the prime ideals in K above q are inert in L. Also, $41^9 \not\equiv \pm 1 \bmod 190$ and $41^{18} \equiv 1 \bmod 190$, so $f^q_{K^+/\mathbb{Q}} = 18$ and hence $g^q_{K^+/\mathbb{Q}} = 2$, so complex conjugation doesn't fix the primes in K above q, and q meets the conditions of Theorem 2. Factor the 190th cyclotomic polynomial modulo 41 to find generators of the prime ideals, and taking a polynomial factor with integer coefficients, up to subtraction by 41, evaluating at ζ_{190}, and dividing by its complex conjugate gives a fractional unit-magnitude non-norm element γ and CDA $\mathcal{A} = (L/K, \theta, \gamma) = (\mathbb{Q}(\zeta_{190}, \zeta_{11} + \zeta_{11}^{-1})/\mathbb{Q}(\zeta_{190}), \theta, \gamma)$, with $[\mathcal{A} : \mathbb{Q}] = 1800$.

CLWE and Non-norm Elements We then apply this result to cryptography. Learning with Errors (LWE) is a cryptographic problem believed to be quantum secure, informally defined as follows: to create an LWE sample, take a secret $s \in \mathbb{Z}_q^n$ for some prime q, sample $a \leftarrow U\left(\mathbb{Z}_q^n\right)$ and an error e according to some distribution, and output $(a, b) = (a, as + e)$. A solver has to find s (equivalently e) or distinguish such samples from uniformly chosen samples; these are the search and decision problems respectively. LWE was introduced by Regev in [7].

To achieve tradeoffs between efficiency and security, structured forms of LWE have been introduced, using algebraic structures such as polynomial rings [5] and modules [4]. In [2], LWE was structured using ideals in CDAs (CLWE). LWE and its variants have reductions from lattice problems which are considered infeasible to solve, such as the shortest vector problem (SVP).

A maximal order is a discrete subring of $\mathcal{A}$ that contains a K-basis of $\mathcal{A}$, and is maximal with respect to inclusion. In the rest of this abstract, $\mathcal{O}$ will denote a maximal order and $\mathcal{I}$ an ideal of $\mathcal{O}$. We embed ideals into $\mathbb{R}^{nd^2}$ as follows. Consider a CDA $\mathcal{A} = (L/K, \theta, \gamma)$ with $[L : K] = d$ and $\gamma = \frac{a}{b} \in K \setminus \mathcal{O}_K$ such that $|\gamma| = 1$. Fixing the L-basis of $\mathcal{A}$, $\{u^i\}_{i \geq 0}$, express an element x as the linear map $\phi(x)$ given by left multiplication on the u^i. For example, if $x = \oplus_{i=0}^{d-1} u^i x_i \in \mathcal{A}$,

$$\phi(x) = \begin{pmatrix} x_0 & \gamma\theta(x_{d-1}) & \dots & \gamma\theta^{d-1}(x_1) \\ x_1 & \theta(x_0) & \dots & \gamma\theta^{d-1}(x_2) \\ \dots & \dots & \dots & \dots \\ x_{d-1} & \theta(x_{d-2}) & \dots & \theta^{d-1}(x_0) \end{pmatrix}.$$

Denote one of the embeddings $K \hookrightarrow \mathbb{C}$ extended to an embedding of L by α. All nd embeddings of L are obtained from the set $\{\alpha \circ \theta^i\}_{\alpha,i}$. We form a vector in $\mathbb{R}^{nd^2}$ from x by concatenating the vectorized images of $\alpha(\phi(x))$ for all $\alpha \in \mathrm{Emb}(K)$. Then any discrete additive group of $\mathcal{A}$ maps to a lattice in $\mathbb{R}^{nd^2}$. We define norms on $\mathcal{A}$: set $\|x\|^2 = \sum_{\alpha \in \mathrm{Emb}(K)} \sum_{i,j} |\alpha(\phi(x)_{i,j})|^p$, and $\|x\|_\infty = \max_{\alpha,i,j} |\alpha(\phi(x)_{i,j})|$, where $\phi(x)_{i,j}$

denotes the i,jth entry of $\phi(x)$. Since γ is unit magnitude, factors of γ appearing in $\phi(x)$ vanish under the above norms, and $\|\cdot\|$ is submultiplicative.

Let the trace $\mathrm{Tr}(\cdot)$ of $x \in \mathcal{A}$ be defined $\mathrm{Tr}(x) = T_{K/\mathbb{Q}} \circ \mathrm{trace}(\phi(x))$, where $T_{K/\mathbb{Q}}$ is the field trace. This is symmetric. The dual of $\mathcal{I}$ is $\mathcal{I}^\vee = \{x \in \mathcal{A} : \mathrm{Tr}(x\mathcal{I}) \subset \mathbb{Z}\}$. We then define the lattice problems we reduce to our variant of CLWE:

Definition 1. Let $\mathcal{I} \subset \mathcal{O}$, $0 < \delta < \lambda_1(\mathcal{I})/2$, and $\xi \geq 1$. The (approximate) Shortest Independent Vectors problem, SIVP_ξ, on $\mathcal{I}$ is to find nd^2 linearly independent non-zero vectors $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ such that $\max_i (\|\boldsymbol{x}_i\|) \leq \xi \cdot \lambda_n(\mathcal{I})$. The $\mathcal{A}-\mathrm{DGS}_r$ problem is to sample a discrete Gaussian $D_{\mathcal{I},r}$ for given r. The $\mathcal{A}$-$\mathrm{BDD}_{\mathcal{O},\mathcal{I},\delta}$ problem, given $y = x+e$ for $x \in \mathcal{I}$ and $e \in \bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}$ satisfying $\|e\| \leq \delta$, is to find x. The $q\mathcal{A}$-$\mathrm{BDD}_{\mathcal{O},\mathcal{I},d}$ problem is, given $\mathcal{A}$-$\mathrm{BDD}_{\mathcal{O},\mathcal{I},\delta}$ instance $y = x + e$, find $x \bmod q\mathcal{I}$.

By [7, Lemma 3.5], for any $q \geq 2$ and $\mathcal{I} \subset \mathcal{O}$, there is a deterministic polynomial time reduction from $\mathcal{A}$-$\mathrm{BDD}_{\mathcal{O},\mathcal{I},\delta}$ to $q\mathcal{A}$-$\mathrm{BDD}_{\mathcal{O},\mathcal{I},\delta}$.

CLWE and the Hardness of Search We then define the CLWE distribution analogously to [2]. There CLWE was defined for a specific order in a family of algebras, the natural order. We define CLWE for arbitrary maximal orders:

Definition 2. Let K be cyclotomic, and $\mathcal{A} := (L/K, \theta, \gamma)$ a cyclic algebra with u: $u^d = \gamma \in K \setminus \mathcal{O}_K$, and $[L : K] = d$ with $\mathrm{Gal}(L/K) = \langle\theta\rangle$. Let $\mathcal{O} \subset \mathcal{A}$. For an error distribution ψ over $\oplus_{i=0}^{d-1} u^i L_{\mathbb{R}}$, prime $q \geq 2$, and $s \in \mathcal{O}_q^\vee$, a sample from CLWE distribution $\Pi_{\mathcal{O},q,s,\psi}$ is obtained by sampling $a \leftarrow U(\mathcal{O}_q)$, $e \leftarrow \psi$, and outputting $(a, b) = (a, (a \cdot s)/q + e \bmod \mathcal{O}^\vee) \in \mathcal{O}_q \times (\oplus_{i=0}^{d-1} u^i L_{\mathbb{R}})/\mathcal{O}^\vee$.

Search CLWE Let Ψ be a family of error distributions over $\bigoplus_{i=0}^{d-1} u^i L_{\mathbb{R}}$. Search CLWE, $\mathrm{CLWE}_{\mathcal{O},q,s,\psi}$, is to recover s from a collection of independent samples from $\Pi_{\mathcal{O},q,s,\psi}$ for any $s \in \mathcal{O}_q^\vee$ and $\psi \in \Psi$.

For the above definition of CLWE, we obtain a reduction from SIVP on maximal order ideal lattices to search CLWE. We require a 'clearing out ideals' lemma. For ideals in arbitrary maximal orders, we have the following, where $\mathrm{ass}(\mathcal{I}) = \{\mathcal{P}_i : \mathcal{I} \subset \mathcal{P}_i\}$ are the *associated primes* of $\mathcal{I}$, and the $\mathcal{P}_i$ are prime ideals of $\mathcal{O}$:

Lemma 4. *Let $\mathcal{I} \subset \mathcal{O}$ and $\mathcal{J}$ be an arbitrary integral ideal of $\mathcal{O}$. Then, there exists an element $t \in \mathcal{I} \cap \mathcal{O}_K$ such that the ideal $t \cdot \mathcal{I}^{-1} \subset \mathcal{O}$ is coprime to $\mathcal{J}$, and we can compute such a t efficiently given $\mathcal{I}$ and $\mathrm{ass}(\mathcal{J})$.*

Proof. Let $\{\mathcal{P}_i\}_{i=1,\ldots,r} = \mathrm{ass}(J)$ and $t \in (\mathcal{I} \setminus \bigcup_i \mathcal{P}_i\mathcal{I}) \cap \mathcal{O}_K$. Suppose $t \cdot \mathcal{I}^{-1} + \mathcal{J} \neq \mathcal{O}$. So $t \cdot \mathcal{I}^{-1} + \mathcal{J} \subset \mathcal{M}$ for maximal ideal $\mathcal{M} \subset \mathcal{O}$. But maximal ideals are prime, so $t \cdot \mathcal{I}^{-1}$ is contained in an associated prime of $\mathcal{J}$. This implies that $t \in \mathcal{P}_i\mathcal{I}$ for some $\mathcal{P}_i \in \mathrm{ass}(\mathcal{J})$. This is a contradiction. To construct such a t, take an $\mathcal{O}_K$ element in $\mathcal{I} \setminus \mathcal{P}_i\mathcal{I}$ for all i, and compute the preimage under the CRT. □

We then prove the 'clearing out ideals' lemma in the standard way:

Lemma 5. *Let $\mathcal{I}, \mathcal{J} \subset \mathcal{O}$ and $t \in \mathcal{I} \cap \mathcal{O}_K$ such that $t \cdot \mathcal{I}^{-1}$ and $\mathcal{J}$ are coprime, and let $\mathcal{P}$ be an arbitrary fractional ideal of $\mathcal{O}$. Then the map $\chi_t : \mathcal{A} \to \mathcal{A}$ defined $\chi_t(x) = t \cdot x$ induces a module isomorphism $\mathcal{P}/\mathcal{J} \cdot \mathcal{P} \to \mathcal{I} \cdot \mathcal{P}/\mathcal{I} \cdot \mathcal{J} \cdot \mathcal{P}$. Furthermore, if $\mathcal{J} = \langle q \rangle$ for an unramified prime $q \in \mathbb{Z}$ we can efficiently compute the inverse.*

The below result is the key application of the 'clearing out ideals' lemma:

Lemma 6. *Let $\mathcal{A} = (L/K, \theta, \gamma)$ be as above and $\mathcal{O} \subset \mathcal{A}$. There is a ppt. algorithm that given unramified $q \geq 2$, invertible fractional ideal $\mathcal{I}^\vee$, a $q\mathcal{A}$-$BDD_{\mathcal{O},\mathcal{I}^\vee,\alpha q \cdot \omega(\sqrt{\log(nd)})/\sqrt{2nd}\cdot r}$ instance $y = x + e$, $r \geq \sqrt{2}q \cdot \eta(\mathcal{I})$, and $D_{\mathcal{I},r'}$ samples with $r' \geq r$, outputs samples within negligible statistical distance of the CLWE distribution $\Pi_{\mathcal{O},q,s,\Sigma}$ for $s = \chi_t\left(x \bmod q\mathcal{I}^\vee\right) \in \mathcal{O}_q^\vee$, where χ_t is as in Lemma 5 and Σ is an error distribution such that if $|\gamma| = 1$ the resulting error e'' has Gaussian marginal distribution in its i, j^{th} coordinate with $r_{i,j} \leq \alpha$.*

Proof. Mutatis mutandis the same as in [2], using our Lemma 5. □

Combining Lemma 6 and an adaptation of [7, Lemma 3.14], we arrive at

Theorem 3. *Given $CLWE_{\mathcal{O},q,\Sigma_\alpha}$ oracle for input $\alpha \in (0,1)$, $q \geq 2$, an ideal $\mathcal{I} \subset \mathcal{O}$, a number $r \geq \sqrt{2}q \cdot \eta(\mathcal{I})$ satisfying $r' := r \cdot \omega(\sqrt{\log N})/(\alpha q) > \sqrt{2N}/\lambda_1\left(\mathcal{I}^\vee\right)$, and polynomially many samples from the discrete Gaussian $D_{\mathcal{I},r}$ there exists an efficient quantum algorithm that outputs an independent sample from $D_{\mathcal{I},r'}$.*

Combining this with a known reduction from SIVP to DGS, we conclude with

Corollary 3. *Let $\mathcal{A}, \mathcal{O}, \alpha$ and q be as above. Then there is a polynomial-time quantum reduction from $\mathcal{A}$-$SIVP_\xi$ to $CLWE_{\mathcal{O},q,\Sigma_\alpha}$ for any $\sqrt{8Nd} \cdot \xi = (\omega(\sqrt{dn})/\alpha)$.*

References

[1] A.A. Albert. *Structure of Algebras*. AMS colloquium publications v. 24. American Mathematical Society, 1939. ISBN: 9780821810248.

[2] C. Grover et al. "Non-commutative Ring Learning with Errors from Cyclic Algebras". In: *Journal of Cryptology* 35.3 (2022), p. 22. DOI: 10.1007/s00145-022-09430-6.

[3] C. Hollanti, J. Lahtonen, and H.-F. Lu. "Maximal Orders in the Design of Dense Space-Time Lattice Codes". In: *IEEE Transactions on Information Theory* 54.10 (2008), pp. 4493–4510. DOI: 10.1109/TIT.2008.928998.

[4] A. Langlois and D. Stehlé. "Worst-case to average-case reductions for module lattices". In: *Designs, Codes and Cryptography* 75.3 (2015), pp. 565–599. ISSN: 1573-7586. DOI: 10.1007/s10623-014-9938-4.

[5] V. Lyubashevsky, C. Peikert, and O. Regev. "On Ideal Lattices and Learning with Errors over Rings". In: *Advances in Cryptology – EUROCRYPT 2010*. Ed. by H. Gilbert. Springer Berlin Heidelberg, 2010, pp. 1–23.

[6] B. A. Sethuraman P. Elia and P. Vijay Kumar. "Perfect Space-Time Codes for Any Number of Antennas". In: *IEEE Transactions of Information Theory* 53 (2007), pp. 3853–3868.

[7] O. Regev. "On lattices, learning with errors, random linear codes, and cryptography". In: *Journal of the ACM* 56 (6 2009). DOI: 10.1145/1568318.

[8] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar. "Full-diversity, high-rate space-time block codes from division algebras". In: *IEEE Transactions on Information Theory* 49.10 (2003), pp. 2596–2616.

[9] Kiran T. and B. Sundar Rajan. "STBC-Schemes with Nonvanishing Determinant for Certain Number of Transmit Antennas". In: *IEEE Transactions on Information Theory* 51 (2005), pp. 2984–2992.

[10] R. Vehkalahti et al. "On the Densest MIMO Lattices From Cyclic Division Algebras". In: *IEEE Transactions on Information Theory* 55.8 (2009), pp. 3751–3780. DOI: 10.1109/TIT.2009.2023713.