Semisimple Rings and Radicals in Coding Theory and Cryptography

William Chuang

February 20, 2025

Contents

1 Introduction

In modern **coding theory** and **cryptography**, it is increasingly common to work with *modules over finite rings* or *group algebras*. For example, one might design an error-correcting code over the ring $\mathbb{Z}_4$ or over $\mathbb{F}_q[x]/(f(x))$, or develop a cryptosystem based on the hardness of problems in certain quotient rings (as in lattice-based cryptography like NTRU or Ring-LWE).

In these settings, the structure of the underlying ring can have a profound impact on:

- The classification of code structures (e.g., $\mathbb{Z}_4$-linear codes vs. field-based codes).
- The security assumptions in cryptosystems (e.g., whether invertibility is easy to determine).
- The feasibility of algebraic attacks that exploit ring-specific properties.

A key tool in classifying rings and modules is the notion of **semisimple algebras** and their opposites: rings with nonzero **Jacobson radical**. These lecture notes aim to provide a short, accessible overview of how these concepts can appear in coding theory and cryptography, focusing on finite dimensional (often finite) rings.

2 Recap of Key Definitions: Semisimple Rings and Jacobson Radicals

Definition 2.1 (Semisimple Ring)**.** A (unital) ring R is called *semisimple* if, as a left module over itself, R is a direct sum of *simple* submodules. Equivalently, R is semisimple if $J(R) = 0$, where $J(R)$ is the Jacobson radical.

Definition 2.2 (Jacobson Radical)**.** Let R be a ring (with identity). The *Jacobson radical* $J(R)$ is defined as the intersection of all maximal left ideals of R (equivalently, the intersection of all maximal right ideals). One important property is that $r \in R$ lies in $J(R)$ precisely if r acts *nilpotently* on every simple left R-module.

Over a finite field (or more generally an Artinian ring), a standard theorem (Wedderburn–Artin) tells us that R is semisimple if and only if $R \cong \prod_i M_{n_i}(D_i)$, a direct product of matrix algebras over division rings D_i. Such a decomposition often simplifies problems in coding and cryptography by reducing complicated module structures to direct sums of simple components.

3 Why Semisimplicity and Radicals Matter for Coding Theory

3.1 Linear Codes over Rings

Background. Classical coding theory usually focuses on *linear codes* over finite fields $\mathbb{F}_q$. However, researchers have studied linear codes over finite rings such as $\mathbb{Z}_4$ or $\mathbb{Z}_{p^m}$ because they can yield interesting families of codes with good error-correcting properties (e.g. *Lee distance* codes over $\mathbb{Z}_4$).

Modules over Finite Rings. A linear code C of length n over a ring R can be viewed as an R-submodule of R^n. Analyzing submodules $C \leq R^n$ can be more subtle if R is *not* a field (since R^n is no longer a free module in the same sense if R has zero-divisors). The presence of a *nonzero* Jacobson radical $J(R)$ means that some elements of R act nilpotently on simple modules. In practice, that can complicate decoding or hamper certain dimension arguments.

Semisimple vs. Non-Semisimple. If R happens to be *semisimple* (i.e. $J(R) = 0$), then every R-module, in particular R^n, has a decomposition into simple summands. Submodules C then break down correspondingly. This decomposition can make analysis of *syndrome decoding*, *dual codes*, and *generator matrices* more straightforward. Conversely, if R has a nontrivial radical, certain pathologies (like zero-divisors that kill submodules or codewords) arise, and one must account for radical elements carefully in code design and decoding algorithms.

3.2 Group Algebras and Group Codes

Group Codes. Another approach is to construct codes from *group algebras* $\mathbb{F}_q[G]$, where G is a finite group. A code can be taken as an ideal (or a left ideal, right ideal, etc.) in $\mathbb{F}_q[G]$. In this setting, the structure of $\mathbb{F}_q[G]$ as a ring heavily influences how we classify such codes.

Maschke's Theorem and Semisimplicity. If $\mathrm{char}(\mathbb{F}_q)$ does not divide $|G|$, then $\mathbb{F}_q[G]$ is semisimple (Maschke's theorem). Hence every ideal in $\mathbb{F}_q[G]$ decomposes into a direct sum of minimal ideals, which correspond to irreducible representations of G. This complete reducibility can simplify the enumeration of all possible group codes and their decoding.

When $J(\mathbb{F}_q[G]) \neq 0$. If $p = \mathrm{char}(\mathbb{F}_q)$ divides $|G|$, then $J(\mathbb{F}_q[G]) \neq 0$, the group algebra is no longer semisimple, and one must carefully analyze the radical to understand how it annihilates certain modules. From a coding perspective, radical elements can kill entire submodules, which might yield degenerate or trivial codes unless handled appropriately. Still, group codes in such cases can be interesting (e.g. leading to certain self-orthogonal or special structure codes).

4 Connections to Cryptography

4.1 Ring-Based Cryptosystems

Polynomial-Ring Constructions. Modern cryptography often uses rings of the form $R = \mathbb{F}_q[x]/(f(x))$ or $\mathbb{Z}[x]/(f(x))$ (and sometimes higher-dimensional analogs) for cryptosystems like NTRU, Ring-LWE, and others. While these rings are not always semisimple, they might factor into simpler components (e.g. if $f(x)$ factors over $\mathbb{F}_q$), or might have certain radical properties if $f(x)$ is not square-free.

Invertibility and the Radical. In many ring-based cryptosystems, one needs random elements in R to be invertible with high probability, or one needs to perform sampling in an ideal quotient. If R has a large Jacobson radical, invertibility can be more subtle and might require extra conditions (like picking polynomials coprime to $f(x)$). From a security viewpoint, understanding $J(R)$ can help ensure the distribution of invertible elements is well-understood and not easily attacked.

Structure of Modules in Post-Quantum Cryptography. Certain *lattice-based* or *module-based* cryptosystems rely on the hardness of finding short vectors in modules over polynomial rings. If the ring were semisimple, it might decompose in ways that could (theoretically) simplify attacks, though in practice one chooses $f(x)$ to ensure difficulty of computations. Nonetheless, ring-theoretic classification theorems can help evaluate potential vulnerabilities.

4.2 Secret Sharing and Zero-Divisors

Some secret sharing schemes or threshold cryptography protocols rely on polynomials over rings with zero-divisors. A nontrivial radical $J(R)$ might allow certain *collisions* or *annihilation effects* that compromise security if not designed properly. For instance, an element $r \in J(R)$ might map multiple distinct codewords (or shares) to the same outcome. By contrast, if R is semisimple, these pathologies cannot occur in the same way because $J(R) = 0$.

5 Illustrative Example: Codes Over $\mathbb{Z}_4$

Why $\mathbb{Z}_4$? One of the simplest examples of a ring with a nonzero radical is $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ under addition and multiplication mod 4. The element 2 is a zero-divisor: $2 \cdot 2 = 0 \pmod 4$. In fact, $J(\mathbb{Z}_4) = \langle 2 \rangle = \{0, 2\}$ is nonzero.

Code Structure. A *linear code* C of length n over $\mathbb{Z}_4$ is a submodule of $(\mathbb{Z}_4)^n$. One can classify such codes, but the presence of 2 as a nilpotent element (since $2 \cdot 2 = 0 \pmod 4$) means that some submodules can be annihilated by 2, leading to interesting code properties. The classical "Gray map" is often used to interpret $\mathbb{Z}_4$-linear codes in terms of binary codes, revealing certain powerful nonlinear codes in $\{0, 1\}^{2n}$.

Decoding and the Radical. Because $2 \in J(\mathbb{Z}_4)$ kills half the elements in the ring (in a sense), the code decomposition is *not* simply a direct sum of irreducibles (since $\mathbb{Z}_4$ is not semisimple). Decoding strategies must account for this radical effect, which can sometimes be exploited to produce good distance properties (e.g. 2 can spread error patterns under the Gray map).

6 Advanced Perspectives and Open Problems

- **Module Decompositions in Quantum-Safe Cryptography:** As post-quantum cryptosystems increasingly rely on ring and module structures, deeper results on radicals and semisimplicity might become relevant. For instance, advanced cryptanalytic techniques might try to exploit ring decompositions or factorization of $f(x)$ in $\mathbb{F}_q[x]$.

- **Non-Semisimple Group Algebras and Code Constructions:** When $p \mid |G|$, $\mathbb{F}_p[G]$ is not semisimple. There remain relatively unexplored questions about systematically constructing error-correcting codes as ideals in $\mathbb{F}_p[G]$ under these conditions, or using such codes in secure communication.

- **Zero-Knowledge Proofs over Rings with Radical:** Some zero-knowledge protocols require proving knowledge of a solution to a linear equation over a ring. If the ring is not semisimple, certain “ghost” components in the radical might provide hidden structures that can be used maliciously (or beneficially) in protocols.

7 Ten Concrete Examples of Nontrivial Radicals in Rings and Their Cryptographic Implications

This section presents ten concrete numeric examples of rings—each with potentially nontrivial Jacobson radicals or specific factorization properties—to illustrate how such structures can open new lines of cryptanalysis or enable novel cryptographic primitives. While these examples are small and mainly serve didactic purposes, they reflect themes that arise in real-world systems at much larger scales.

7.1 $\mathbb{Z}_4$

Ring: $R = \mathbb{Z}_4 = \{0, 1, 2, 3\}$ with addition and multiplication mod 4.

Radical:

$$J(R) = \{0, 2\},$$

since $2 \cdot 2 \equiv 0 \pmod 4$. This shows 2 is nilpotent (of index 2).

Implication: Any cryptographic scheme or linear code over $\mathbb{Z}_4$ must handle the fact that 2 annihilates half of the elements (creating zero-divisors). This can lead to special distance properties in codes (e.g. Gray-mapped $\mathbb{Z}_4$-codes) or vulnerabilities if invertibility is assumed without checking the radical.

7.2 Example 2: $\mathbb{Z}_4[x]/(x^2 + 1)$

Ring: $R = \mathbb{Z}_4[x]/(x^2 + 1)$.

Reasoning: Over $\mathbb{Z}_4$, the polynomial $x^2 + 1$ may factor or remain irreducible mod 2; however, regardless of factorization, $\mathbb{Z}_4$ itself already has a nontrivial radical (see Example 7.1).

Radical: Elements coming from $\overline{2}$ in the quotient remain nilpotent, and $\overline{x}$ could also be radical if $(x^2 + 1)$ is not invertible. Hence $J(R)$ includes images of $\langle 2 \rangle$ (and possibly more).

Implication: A naive cryptosystem using R might require inverting polynomials that become zero-divisors under multiplication by $\overline{2}$. Adversaries could exploit such degeneracies to forge signatures or break encryption schemes that do not carefully avoid the radical.

7.3 Example 3: Field Example (No Radical) $\mathbb{F}_2[x]/(x^2 + x + 1)$

Ring:

$$R = \mathbb{F}_2[x]/(x^2 + x + 1).$$

Since $x^2 + x + 1$ is irreducible over $\mathbb{F}_2$, R is a field of size 4.

Radical:

$$J(R) = \{0\} \quad \text{(fields have zero radical).}$$

Implication: Working over a field is simpler for both coding and cryptography, because every nonzero element is invertible, and there are no zero-divisors. However, field-based approaches may have smaller parameter spaces or other limitations (e.g. limited extension fields).

7.4 Example 4: Small Group Algebra $\mathbb{F}_3[G]$ with $G = \mathbb{Z}_2$

Group: $G = \mathbb{Z}_2$, the cyclic group of order 2.

Ring:

$$R = \mathbb{F}_3[G] \cong \mathbb{F}_3[x]/(x^2 - 1).$$

Factorization: $x^2 - 1 = (x-1)(x+1)$ in $\mathbb{F}_3$. Note that ± 1 are actually the same in $\mathbb{F}_3$, but we still get two distinct factors.

Radical: Since $\text{char}(\mathbb{F}_3)$ does not divide $|G| = 2$, the group algebra is semisimple, so $J(R) = 0$.

Implication: If we switched to $\mathbb{F}_2$ instead, then $\text{char}(2) \mid |G|$, and we would get a nontrivial radical. In group-code constructions, semisimplicity or non-semisimplicity determines how ideals decompose and thus how one can build or classify group codes.

7.5 Example 5: $\mathbb{F}_2[x]/((x+1)^2)$

Ring:

$$R = \mathbb{F}_2[x]/\big((x+1)^2\big).$$

Factorization: $(x+1)$ is irreducible of degree 1 over $\mathbb{F}_2$, but it appears *twice* in the polynomial $(x+1)^2$.

Radical: $\langle \overline{x+1} \rangle$ is nilpotent in the quotient, so

$$J(R) = \langle \overline{x+1} \rangle.$$

Implication: This ring is not a field. A cryptosystem using R must handle collisions or zero-divisors arising from $\overline{x+1}$. This might allow certain short-vector or collision attacks if the system design assumes invertibility beyond what actually holds in the radical.

7.6 Example 6: $\mathbb{F}_5[x]/\big((x^2 + 2x + 2)^2\big)$

Ring:

$$R = \mathbb{F}_5[x]/\big((x^2 + 2x + 2)^2\big).$$

Factorization: $x^2 + 2x + 2$ may or may not factor in $\mathbb{F}_5$. Even if it is irreducible, the square $\big(x^2 + 2x + 2\big)^2$ introduces repeated roots.

Radical: The ideal generated by $\overline{x^2+2x+2}$ is nilpotent, so it is contained in $J(R)$. Indeed, that entire factor forms the radical.

Implication: In a ring-based cryptosystem that tries to invert polynomials in R, the presence of a repeated factor complicates invertibility. Attackers might target polynomials that vanish in the radical to create collisions or to reduce the effective key space.

7.7 Example 7: NTRU-Style Construction with $x^n - 1$

Ring:

$$R = \mathbb{Z}_q[x]/(x^n - 1)$$

for some small prime q. For instance, let $n = 8$ and $q = 17$.

Factorization: $x^8 - 1 = (x^4 - 1)(x^4 + 1)$. Over $\mathbb{F}_{17}$, one checks whether $(x^4 - 1)$ or $(x^4 + 1)$ have repeated factors.

Radical: If either factor has repeated roots mod 17, that factor yields a nontrivial radical. If all factors are distinct and square-free, the ring is closer to semisimple (though not necessarily fully semisimple if the factorization involves irreps of different degrees).

Implication: NTRU-like schemes rely on inverting polynomials in R. Nontrivial radicals mean some elements are noninvertible, potentially leading to special "collisions." Attackers might exploit knowledge of repeated roots or non-trivial radicals to find weaknesses or reduce the effective key space.

7.8 Example 8: A Trapdoor Factorization in $\mathbb{F}_2[x]$

Ring:

$$R = \mathbb{F}_2[x]/\big(f(x)g(x)\big),$$

where $f(x)$ and $g(x)$ are distinct irreducibles of the same degree.

Trapdoor Setup: If the system designer knows the factorization $f(x)g(x)$, but the factorization is not publicly known, one could attempt a "trapdoor" cryptosystem. Over large fields and large degrees, factoring might still be feasible, but in principle this is a classical idea.

Radical: If $f(x)$ or $g(x)$ appear more than once (repeated factor), it contributes to $J(R)$. Otherwise, if each appears exactly once, R might be semisimple.

Implication: The radical could hide partial information about codewords or ciphertexts. Alternatively, if factoring over $\mathbb{F}_2$ is not as hard as intended, an adversary can break the scheme. This example highlights how factorization and radical theory can create or undermine cryptographic trapdoors.

7.9 Example 9: Code-Based Construction in $\mathbb{F}_{2^m}[x]/(x^r - 1)$

Ring:

$$R = \mathbb{F}_{2^m}[x]/(x^r - 1).$$

Factorization: $x^r - 1$ can factor into distinct irreducibles or might have repeated factors. If repeated, those factors yield nontrivial radicals.

Radical: If $(x^r - 1)$ is square-free in $\mathbb{F}_{2^m}[x]$, R is closer to a direct product of irreducible components (hence semisimple). If not, the radical complicates the structure.

Implication: Such rings arise in cyclic or quasi-cyclic code constructions. Code parameters (e.g. minimum distance, dimension) can be simpler to analyze in semisimple cases. Nonsemisimple cases might yield codes with unusual properties or require more intricate decoding algorithms.

7.10 Example 10: $\mathbb{Z}[x]/(x^n + 1)$ mod q with a Known "Hidden" Radical

Ring:

$$\widetilde{R} = \mathbb{Z}[x]/(x^n + 1) \quad \text{then reduce modulo } q,$$

i.e. $R = \big(\mathbb{Z}[x]/(x^n + 1)\big)/\langle q \rangle \cong \mathbb{F}_q[x]/(x^n + 1)$.

Factorization: If $(x^n + 1)$ has repeated roots mod q, it introduces a radical in R.

Implication: Ring-LWE or related lattice-based schemes often require that $x^n + 1$ remain square-free over $\mathbb{F}_q$. If an attacker finds a prime q such that $(x^n + 1)$ factors with repeated roots, they might exploit the radical to break certain cryptographic assumptions. This can act as a specialized *trapdoor prime*.

These ten examples illustrate the interplay between:

- **Nontrivial radicals** (zero-divisors, nilpotent elements, collisions),
- **Semisimplicity** (direct sum decompositions, simpler invertibility),
- **Polynomial factorization** (square-free vs. repeated factors),
- **Cryptographic security** (potential trapdoors, attack surfaces).

Although small, each example shows how ring-theoretic structure can lead to unique advantages or pitfalls in both *coding theory* (distance properties, decoding complexity) and *cryptography* (invertibility, key distribution, collisions). In real-world systems, these issues arise at a much larger scale but remain fundamentally governed by the same algebraic principles.

8 Cryptography Over Rings: NTRU and Ring-LWE

In modern public-key cryptography, especially in the context of *post-quantum* schemes, a major trend is to use polynomial quotient rings in place of classical structures like integer moduli. Two prominent examples are the **NTRU** family of schemes and cryptosystems based on the **Ring-LWE** (Learning With Errors) problem.

8.1 NTRU Cryptosystems

Originally introduced by Hoffstein, Pipher, and Silverman in the 1990s, NTRU relies on the difficulty of finding short vectors in a certain convolution structure. Concretely, one often works in a ring of the form

$$R = \mathbb{Z}[x]/(x^n - 1) \quad \text{or} \quad \mathbb{Z}_q[x]/(x^n - 1),$$

where n is chosen so that polynomial multiplication can be done efficiently. A user's secret key is typically a pair of "small" polynomials (f, g) in R, whereas the public key is a polynomial $h \equiv f^{-1} \cdot g \pmod{q}$ (under some conditions ensuring invertibility). Encryption and decryption exploit the structure of polynomial multiplication in R, along with reduction by a small norm.

Relevance to Ring Theory.

- If $(x^n - 1)$ factors in certain ways or if q is chosen so that R has a nontrivial radical, it can affect the distribution of invertible elements and potentially open avenues for cryptanalysis.
- NTRU's security relies on the hardness of finding short vectors in a lattice associated with R, not just on factorization. However, ring decompositions can sometimes be used to analyze sublattices or subrings.

8.2 Ring-LWE

Introduced by Oded Regev in the context of LWE (Learning With Errors) and later specialized to ring structures by Vadim Lyubashevsky, Chris Peikert, and others, Ring-LWE leverages the idea of adding a "noise term" to polynomial samples in a quotient ring

$$R_q \;=\; \frac{\mathbb{Z}[x]}{\langle f(x)\rangle}\Big/\langle q\rangle \;\cong\; \frac{\mathbb{F}_q[x]}{\langle \overline{f}(x)\rangle},$$

where $f(x)$ is typically chosen to be a polynomial like $x^n + 1$ or $x^n - 1$.

Core Idea. Just as in standard LWE, one has samples of the form

$$(a,\, a \cdot s + e) \;\in\; R_q \times R_q,$$

where s is the secret "short" polynomial (the analog of a secret vector in classical LWE) and e is a small noise polynomial. Distinguishing such samples from uniform random pairs is conjectured to be hard for appropriate choices of $f(x)$ and noise distribution.

Ring-Theoretic Considerations.

- If $f(x)$ is not square-free mod q, R_q may have a nontrivial radical, complicating invertibility or introducing zero-divisors. This can sometimes reduce the security level or force additional constraints on $f(x)$ and q.
- On the other hand, the *algebraic* structure of R_q—especially if it is semisimple—helps keep multiplication efficient and maintain well-defined error growth properties.

8.3 Security and Implementation Details

In both NTRU and Ring-LWE, one key benefit of polynomial quotient rings is *efficiency*:

- Polynomial multiplication can be done via FFT-like algorithms in $O(n \log n)$ time.
- If R is chosen to be semisimple, the ring is more straightforward to analyze; if R has a nontrivial radical, one must ensure it does not enable any "collisions" that compromise security.

Despite these ring-theoretic considerations, the core difficulty typically lies in the *lattice* perspective (finding short vectors in high-dimensional modules). Thus, cryptanalysts often combine ring factorization checks with lattice attacks to probe the full security of such schemes.

8.4 Further Reading

For more in-depth exploration of these ring-based schemes:

- **NTRU:** Original references by Hoffstein, Pipher, and Silverman, or surveys on NTRU. Many open-source libraries implement NTRU variants (e.g. `libpqcrypto`, `OpenQuantumSafe`).
- **Ring-LWE:** Works by Oded Regev, Vadim Lyubashevsky, Chris Peikert, and others, detailing the hardness assumptions and noise analysis. The *CRYSTALS-Kyber* and *NewHope* cryptosystems are examples of Ring-LWE implementations.

In both areas, the **structure of the underlying ring**—whether or not it is semisimple, how polynomials factor, and the nature of its Jacobson radical—can significantly influence security, parameter selection, and performance.

9 Conclusion and Further Reading

Understanding the **Jacobson radical** and **semisimple structures** is not just a pure algebraic pursuit: it has direct ramifications in how codes are designed, how cryptosystems are secured, and how one performs computations with modules over rings. In coding theory, a nonzero radical can lead to codes with special properties (or complications), while in cryptography it can affect invertibility, distribution of keys, or potential algebraic vulnerabilities.

For a deeper dive:

- **Finite Ring Theory:** *Finite Rings with Applications to Combinatorics* by T. Y. Lam provides an accessible treatment of radicals and semisimplicity in finite rings, including examples of $\mathbb{Z}_4$-codes.
- **Group Algebras:** *Representation Theory of Finite Groups* by Benjamin Steinberg (and other texts) discuss how group algebra decompositions relate to coding and representation.
- **Cryptography over Rings:** Surveys on *Ring-LWE* and *NTRU* give a sense of how polynomial quotient rings factor into modern public-key cryptography. Many references (e.g. works by Vadim Lyubashevsky, Chris Peikert, Oded Regev) detail ring-based assumptions in post-quantum cryptography.

Summary of Main Points

- **Semisimple rings** have zero Jacobson radical and decompose into matrix algebras over division rings. This can simplify module structure and code design.
- **Non-semisimple rings** have a nontrivial radical $J(R)$, which can introduce nilpotent elements. This can be beneficial (or problematic) in coding and cryptography, depending on one's design goals.
- **Group algebras and polynomial rings** are prime examples in both coding theory and cryptography, and their semisimplicity depends on characteristic and factorization properties.
- **Practical ramifications** include code performance (distance properties, decoding complexity) and cryptosystem security (invertibility, structural attacks, etc.).

10 References

References

[1] T. Y. Lam, *A First Course in Noncommutative Rings*, Graduate Texts in Mathematics, Vol. 131, Springer, 2001.

[2] T. Y. Lam, *Lectures on Modules and Rings*, Graduate Texts in Mathematics, Vol. 189, Springer, 1999.

[3] N. Jacobson, *Structure of Rings*, American Mathematical Society, 1956.

[4] E. Artin, *Rings with the Minimum Condition*, Univ. of Notre Dame Press, 1953.

[5] D. S. Dummit and R. M. Foote, *Abstract Algebra*, 3rd ed., John Wiley & Sons, 2004.

[6] K. R. Goodearl and R. B. Warfield, *An Introduction to Noncommutative Noetherian Rings*, 2nd ed., Cambridge University Press, 2004.

[7] T. Y. Lam, *Finite Fields and Galois Theory*, 2nd ed., Springer, 2005.

[8] N. Jacobson, *Basic Algebra II*, W. H. Freeman, 1989.

[9] T. Y. Lam, *Introduction to Quadratic Forms over Fields*, Graduate Studies in Mathematics, Vol. 67, American Mathematical Society, 2005.

[10] J. A. Green, *Polynomial Representations of GL(n)*, 2nd ed., Lecture Notes in Mathematics, Vol. 830, Springer, 2007.

[11] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977.

[12] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, 2003.

[13] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and Its Applications, Vol. 20, Cambridge University Press, 1997.

[14] B. Steinberg, *Representation Theory of Finite Groups: An Introductory Approach*, Springer, 2011.

[15] T. Y. Lam, *Lectures on Modules and Rings*, Graduate Texts in Mathematics, Vol. 189, Springer, 1998.

[16] V. Lyubashevsky, C. Peikert, and O. Regev, *On Ideal Lattices and Learning with Errors over Rings*, J. ACM, Vol. 60, No. 6, 2013, Article 43.

[17] J. Hoffstein, J. Pipher, and J. H. Silverman, *NTRU: A Ring-Based Public Key Cryptosystem*, in *Algorithmic Number Theory (ANTS-III)*, LNCS 1423, Springer, 1998, pp. 267–288.

[18] R. Rivest, A. Shamir, and L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Commun. ACM, Vol. 21, No. 2, 1978, pp. 120–126. (See also US Patent 4,405,829)

[19] J. Daemen and V. Rijmen, *AES and the Wide Trail Design Strategy*, in *Lecture Notes in Computer Science*, Vol. 2260, Springer, 2001, pp. 222–238. (See also US Patent 7,064,758)

[20] G. Brassard, *Modern Cryptology: A Tutorial*, LNCS 325, Springer, 1988.

[21] D. Boneh and G. Durfee, *Cryptanalysis of RSA with Private Key $d < N^{0.292}$*, IEEE Trans. Inform. Theory, Vol. 46, No. 4, 2000, pp. 1339–1349.

[22] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 3rd ed., CRC Press, 2020.

[23] D. Micciancio and S. Goldwasser, *Complexity of Lattice Problems: A Cryptographic Perspective*, Kluwer Academic Publishers, 2002.

[24] O. Goldreich, *Foundations of Cryptography, Vol. 2: Basic Applications*, Cambridge University Press, 2004.

[25] S. Galbraith, *Mathematics of Public Key Cryptography*, Cambridge University Press, 2012.

[26] P. Garrett, *Making, Breaking Codes: Introduction to Cryptology*, 2nd ed., Pearson/Prentice Hall, 2005.

[27] S. A. Amitsur, *Radicals of Rings and Their Applications*, in *Proc. Symposia in Pure Math.*, Vol. 24, American Mathematical Society, 1971.

[28] R. Baer, *Linear Algebra and Projective Geometry*, Academic Press, 1952.

[29] G. Cohen, S. Litsyn, A. Lobstein, and G. Zémor, *Issues in Coding Theory*, World Scientific, 2000.

[30] P. Trifonov, *Randomized Concatenation of Polar Codes*, IEEE Trans. Inform. Theory, Vol. 66, No. 6, 2020, pp. 3578–3597.