Journal of Libyan Academy Bani Walid 2025
مجلة الأكاديمية الليبية بني وليد
e-ISSN: 3104-3860
المجلد الأول، العدد الثاني، 2025

دراسة تطبيقية حول الحلقات الجبرية ونظرية الرموز : مدخل حديث للتشفير الكمي

ام الخيرسالم المبروك بليبلو *
قسم الرياضيات، كلية العلوم الصحية – العجيلات ، جامعة الزاوية، ليبيا.
*البريد الإلكتروني (للباحث المرجعي): o.bleblou@zu.edu.ly

An Applied Investigation of Algebraic Rings and coding theory: A modern perspective on Quantum cryptography

Omalkhear Salem Blabulo *
Department of Mathematics, Faculty of science -Aleajilat, University of Zawia, Libya.

Received: 22-02-2025; Accepted: 14-04-2025; Published: 30-05-2025

الملخص
يتناول هذا البحث استخدام الحلقات الجبرية ونظرية الرموز كمدخل حديث لتطوير أنظمة التشفير المقاومة للهجمات الكمومية .مع تطور تقنيات الحوسبة الكمومية أصبحت أنظمة التشفير التقليدية مهددة ، مما استدعى التوجه نحو بنى رياضية أكثر تعقيدا مثل الحلقات الجبرية . أستعرض البحث المفاهيم الأساسية للحلقات الجبرية ونظرية الرموز ثم تناول تطبيقها في بناء نظام التشفير NTRUوهو أحد الأنظمة التي تعتمد على الحلقات متعددة الحدود، خلص البحث إلى أن استخدام الحلقات الجبرية في التشفير يوفر أداء عاليا وأمانا قوياً ضد التهديدات الكمومية مع إمكانية تطوير أنظمة أكثر تقدمًا مستقبلا عبر دمج هذا النهج مع الذكاء الاصطناعي والشبكات الذكية.

الكلمات الدالة: نظرية الرموز، الحلقات الجبرية، التشفير الكمي، التشفير بعد الكم، الحوسبة الكمومية.

Abstract
This research explores the use of algebraic rings and coding theory as framework for constructing cryptographic systems that are secure against quantum threats. As quantum computing continues to evolve, classical encryption methods like RSA and ECC are becoming increasingly vulnerable to quantum algorithms, especially Shor's algorithma modern mathematical.
The study focuses on the theoretical foundations of ring structures and error-correcting codes, emphasizing their practical application in designing quantum-resistant encryption algorithms. A key focus is the NTRU cryptosystem, which is based on polynomial rings and is recognized for its efficiency and resilience to quantum attacks.
A simplified Python implementation of NTRU is provided to demonstrate the encryption and decryption processes using algebraic ring operations. The research confirms that these structures offer a powerful and efficient basis for post-quantum cryptography.

Keywords: Abstract algebra, coding theory, quantum cryptography, quantum computing, ring-based encryption.

المقـدمـــــة

يشهد العالم اليوم طفرة في تقنيات الحوسبة الكمومية، التي باتت تهدد العديد من أنظمة التشفير الكلاسيكية المعتمدة منذ عقود، أمام هذا التحدي تبرز الحادة الملحّة لتطوير أساليب تشفير جديدة، قادرة على الصمود

أمام قدرات الحواسيب الكمومية المتزايدة، في هذا الإطار، تمثل الحلقات الجبرية ونظرية الرموز مجالاً واعداً لتصميم أنظمة تشفير قوية وآمنة.
لقد اثبتت الحلقات الجبرية – بمرونتها وغناها البنيوي – قدرتها على تشكيل بيئة رياضية مناسبة لبناء خوارزميات تشفير حديثة مثل NTRV التي أظهرت مقاومة كبيرة للهجمات الكمومية الى جانب كفاءتها العالية.
من خلال هذا البحث نسعى إلى تسليط الضوء على الأسس النظرية لهذه الحلقات وشرح كيفية توظيفها في تصميم أنظمة تشفير حديثة، مع تقديم دراسة تطبيقية مدعومة بنتائج فعلية، نأمل أن يساهم هذا العمل في فتح آفاق جديدة للبحث في هذا المجال الحيوي بما يواكب التحديات الأمنية المتوقعة في عصر الحوسبة الكمومية.

1.2 مشكلة البحث

رغم وفرة الدراسات التي تناولت الحلقات الجبرية ونظرية الرموز كلٍ على حدة، إلا أن الدراسات التي تعالج العلاقة بينهما في إطار التشفير الكمي ما تزال محدودة.
من هنا تنبع مشكلة هذا البحث، والتي يمكن صياغتها بالسؤال الآتي:-
إلى أي مدى يمكن توظيف الحلقات الجبرية في بناء شفرات مقاومة للتشفير الكمي، من خلال نظرية الرموز؟

1.3 أسئلة البحث

1- ما الخصائص الجبرية للحلقات التي تسهم في تصميم شفرات فعّالة؟
2- كيف تساهم الحلقات الجبرية في تطوير نظرية الرموز؟
3- ما هي أوجه التفاعل بين البنية الجبرية والتشفير الكمي؟
4- هل يمكن تقديم نموذج عملي لشيفرة مبنية على حلقة جبرية تقاوم الهجمات الكمية؟

1.4 أهداف البحث

1- استعراض المفاهيم الأساسية في الحلقات الجبرية ونظرية الرموز.
2- تحليل إمكانيات استخدام الحلقات الجبرية في بناء الشفرات.
3- مناقشة العلاقة بين الجبر المجرد والتشفير الكمي.
4- تقديم نموذج تطبيقي لشيفرة مبنية على بنية حلقة محددة.

1.5 أهمية البحث

علمية : يساهم في سد فجوة بحثية تربط بين الجبر المجرد والتطبيقات التشفيرية الحديثة.
عملية : يمهد الطريق لتطوير أنظمة تشفير مستقبلية مقاومة للهجمات الكمومية.
أكاديمية : يعزز التكامل بين فروع الرياضيات النظرية والتطبيقات الحاسوبية.

1.6 حدود البحث

يركز البحث على الحلقات التبادلية المحدودة وتطبيقاتها في نظرية الرموز الخطية.
يتناول جانباً نظرياً وتحليلياً، ولا يشمل برمجة عملية لخوارزميات التشفير الكمي.

1.7 منهجية البحث

يعتمد البحث على المنهج التطبيقي لأنه لا يكتفي بشرح النظريات فقط بل يطبقها في نموذج عملي .
حيث تم استخدام الأدوات التالية في تنفيذ الدراسة
- البرمجة بلغة Python: لتنفيذ نموذج تشفير يعتمد على الحلقات الجبرية .
- مفاهيم الجبر المجرد : خاصة الحلقات متعددة الحدود
- مقارنة نظرية : بين نظام التشفير المقترح (NTRU)وأنظمة تقليدية مثل RSA, ECC
-تحليل بسيط للنتائج: من حيث الكفاءة والسرعة ومستوى الأمان
- تمت الدراسة وفق هده الخطوات :

1- اختيار نموذج رياضي $zq[x]/(xn-1)$
2- إعداد الكود البرمجي لتوليد مفاتيح التشفير وفك التشفير .
3- تجربة الكود باستخدام قيم محدودة ومعقولة.
4- تسجيل النتائج وتحليلها من حيث الكفاءة والأمان .
5- مقارنة النتائج مع أنظمة تشفير معروفة .

1.8 هيكل البحث

يتكون هذا البحث من ستة فصول يشمل الإطار العام والمفاهيم الأساسية في الجبر ونظرية الرموز، وتحليل العلاقة بين الحلقات الجبرية والتشفير الكمي.
ثم دراسة تطبيقية ونموذج مقترح، وأخير النتائج والتوصيات.

الفصل الثاني : الخلفية النظرية في الحلقات الجبرية

2.1 تمهيد :

تعد الحلقات الجبرية إحدى الركائز الأساسية في الجبر المجرد وقد ظهرت في سياق تعميم مفهوم الأعداد الصحيحة لتكوين بنى رياضية أكثر شمولاً.
تتميز الحلقات بخصائص هيكلية تتيح إجراء عمليات رياضية منظمة، وهو ما جعلها أساساً لتطبيقات متعددة في مجالات الترميز، التشفير، نظرية الحوسبة.
في هذا الفصل سيتم عرض الإطار النظري المرتبط بالحلقات، مع بيان خصائصها وأنواعها وتطبيقاتها.

2.2 تعريف الحلقة الجبرية

تعرف الحلقة (Ring) بأنها مجموعة R مزودة بعمليتين ثنائيتين : الجمع + والضرب.
تحقق الخصائص التالية :

1- الإغلاق تحت الجمع والضرب لكل $a, b \epsilon R$ فإن $a + b \epsilon R, a.b \epsilon R$
2- $(+, R)$ مجموعة إبدالية (Abelian Group) :

أي أن الجمع تبادلي، تجميعي ويحتوي على عنصر محايد وعناصر معكوسة.

3- الضرب تجميعي :

$$(a.b).c = a.(b.c)$$

4- التوزيع لكل $a, b, c, \epsilon r$

$$a.(b+c) = a.b + a.c \quad \ldots\ldots\ldots (1)$$
$$(a+b).c = a.c + b.c \quad \ldots\ldots\ldots (2)$$

2.3. انواع الحلقة الجبرية

2.3.1 الحلقات التبادلية

(Commutative Rings)

حلقات يكون فيها الضرب تبادليا، أي $ab = ba$ تستخدم بكثرة في نظرية الرموز.

2.3.3 الحلقات النمطية

(Modular Riugs)

حلقات تكون معرفة على الشكل Zn وتستخدم على نطاق واسع في التشفير الكلاسيكي والحديث.

2.3.4 الحلقات بدون قواسم صفرية (Integral Domains)

حلقة تبادلية تحتوي على عنصر محايد ولا تحتوي على قواسم صفرية، أي لا يوجد $a, b \neq 0$ بحيث $ab = 0$.

2.4 أمثلة على الحلقات:

* حلقة الأعداد الصحيحة : Z أشهر مثال على الحلقة تبادلية ذات وحدة.
*الحلقة النمطية :Zn مهمة في الترميز والتشفير خاصة إذا كان n عدداً أولياً.
*حلقة المصفوفة Mn (IR) : حلقة غير تبادلية تستخدم في التطبيقات الهندسية.

2.5 تطبيقات الحلقات في الرياضيات والتشفير:

2.5.1 في نظرية الاعداد

تستخدم الحلقات في دراسة القواسم المودول والمجالات.

2.5.2 في نظرية الرموز

تستخدم الحلقات لبناء شفرات خطية ومعقدة مثل شفرات Reed – Solomon وشفرات BCH

2.5.3 في التشفير الكلاسيكي والبعد - الكمومي

الحلقات تستخدم كأساس لبناء خوارزميات مقاومة لهجمات الحوسبة الكمية، مثل التشفير المعتمد على الحلقات النمطية (Lattice – based cryptography)

2.6 مقارنة بين الحلقات والمجالات والحقول:

جدول 1: مقارنة بين الحلقات والمجالات والحقول.

الخاصية	الحلقة	المجال	الحقل
الضرب تبادلي؟	ليس دائماً	نعم	نعم
وجود وحدة؟	ليس دائماً	نعم	نعم
قواسم صفرية؟	ممكن	لا	لا
القسمة ممكنة	لا	لا دائما	نعم

الفصل الثالث : نظرية الرموز وتطبيقاتها الجبرية

3.1 تمهيد :

تمثل نظرية الرموز (Coding theory) أحد أهم فروع الرياضيات التطبيقية حيث تهدف إلى تصميم شفرات قادرة على الكشف عن الأخطاء وتصحيحها أثناء نقل أو تخزين البيانات وقد تطورت هذه النظرية من أسس عددية وجبرية لتصبح أساساً في أنظمة الاتصالات وأمن المعلومات ومع تطور المتطلبات الأمنية في العصر الرقمي ازدادت أهمية توظيف البنى الجبرية – وخصوصاً الحلقات – لتصميم شفرات أكثر كفاءة ومتانة.

3.2 المفاهيم الأساسية في نظرية الرموز :

3.2. 1 الشفرة (Code):

مجموعة جزئية من مجموعة رسائل يمثل كل عنصر منها كلمة بكلمة تسمى (كلمة مشفرة).

3.2.2 الشفرات الخطية (Linear Codes) :

هي شفرات تكون فيها مجموعة الكلمات المشفرة فضاءً جزئياً جبرياً (subspace) من فضاء متجهات على حقل أو حلقة.

3.2.3 الطول (Length) والبعد (Dimension) :

الطول : عدد الرموز في كل كلمة مشفرة.

البعد : عدد المتجهات المولدة للفضاء الجزئي الذي تمثل الشيفرة.

3.2.4 الوزن (weight) :

عدد الرموز غير الصفرية في الكلمة المشفرة. يستخدم لحساب قدرة الشفرة على كشف وتصحيح الأخطاء.

3.3 أمثلة على الشفرات الكلاسيكية :

3.3.1 شيفرة Hamming :
شفرة خطية بسيطة قادرة على تصحيح خطأ واحد وكشف خطأين.
3.3.2 شيفرة Reed - Solomon :
تستخدم على نطاق واسع في الأقراص المضغوطة وأنظمة الأقمار الصناعية.
3.3.3 شفرات BCH :
قوية في تصحيح الأخطاء ويمكن التحكم بدرجة تصحيح الخطأ مسبقاً.
3.4 الرموز فوق الحلقات (Codes Over Rings) :
ظهرت الشفرات المبنية على الحلقات كامتداد للشفرات الخطية التقليدية المبنية على الحقول ومن بين أشهر الحلقات المستخدمة في بناء هذه الشفرات تستخدم في تصميم شفرات رمزية:

Z4.

$$Fq[X]/\ f(x).$$

تلعب دوراً مهماً في تشفير البيانات.
الفوائد :
مرونة أعلى في بناء الشفرات
إمكانية تصميم شفرات غير خطية ذات أداء محسن.
دعم التشفير بعد – كمومي (Post – Quantum Cryptography)
3.5 العلاقة بين نظرية الرموز والحلقات الجبرية :
3.5.1 بنية الشفرات :
يبنى الفضاء الشفري عادة كوحدة (Module) على حلقة ما يوفر أدوات تحليل أقوى من الفضاءات المتجهة التقليدية.
3.5.2 تحليل الأخطاء :
تمكن خواص الحلقة (مثل القواسم الصفرية أو وجود وحدة) من فهم أعمق لقدرة الشيفرة على التعامل مع أخطاء متعددة.
3.5.3 التشفير الكمي :
نظراً لتغير التحديات الأمنية، أصبحت الشفرات المبنية على حلقات تمثل أساساً لتصميم شفرات مقاومة للهجمات الكمومية عبر استغلال مشاكل جبرية معقدة يصعب حلها حتى بالحوسبة الكمية.
3.6 شفرات Post – Quantum وعلاقتها بالحلقات :
يتم حالياً أنظمة تشفير تعتمد على مشاكل صعبة مثل :
مشكلة فك الشيفرة الخطية (LPN Problem) فوق حلقات معينة
مشاكل Lattice في الحلقات النمطية المستخدمة في خوارزميات مثل NTRU
امثلة حديثة :
شفرة TrueCrypt : تعتمد على كثيرات الحدود في حلقة معيارية.
شفرة Ring-Lowe : تستخدم تحويلات بين حلقات توليد مفاتيح تشفير قوية.

الفصل الرابع :
التشفير الكمي ودور الحلقات الجبرية في تصميم شفرات مقاومة له
4.1 تمهيد :

أدى التطور المتسارع في تقنيات الحوسبة الكمية الى ظهور تحديات جديدة في مجال أمن المعلومات. إذ إن العديد من خوارزميات التشفير التقليدية. مثل RSA وECC تعتمد في أمانها على صعوبة مسائل رياضية يمكن حلها بكفاءة بواسطة الحواسيب الكمية استجابة لهذه التهديدات.

ظهر ما يعرف بالتشفير بعد – الكمومي Post-Quantum Cryptography

الذي يعتمد على مشاكل رياضية مقاومة للحوسبة الكمية.

ومن بين الهياكل الجبرية الواعدة في هذا المجال : الحلقات الجبرية.

4.2 الحوسبة الكمية والتحديات الأمنية :

4.2.1 مبدأ الحوسبة الكمية :

تعتمد الحواسيب الكمية على مفاهيم فيزيائية مثل التراكب والتشابك وتستعمل وحدات معلومات تعرف بالبتات الكمية (Qubits) مما يمنحها القدرة على معالجة عدد كبير من الحالات في وقت متزامن.

4.2.2 خوارزميات التهديد :

خوارزمية Shor : تكسر RSA وESDSA بكفاءة.

خوارزمية Grover : تسرع عمليات البحث العشوائي. ما يهدد خوارزميات المفاتيح المتماثلة.

النتيجة : الحاجة لتصميم أنظمة تشفير جديدة تقاوم الحوسبة الكمية.

4.3 التشفير بعد الكمومي (post – Quantum Cryptography) :

هو مجال تطوير أنظمة تشفير تعتمد على مسائل رياضية يعتقد أنها صعبة حتى على الحواسيب الكمية وتشمل هذه الأنظمة :

التشفير المعتمد على الشفرات (Code – based).

التشفير الشبكي (Lattice – based).

التشفير متعدد المتغيرات (Multivariate).

التشفير باستخدام الحلقات و الموديلات (Ring – based Cryptography).

4.4 دور الحلقات الجبرية في التشفير الكمي :

4.4.1 بيئة غنية رياضياً :

توفر الحلقات إطاراً مرناً يمكن من خلاله تمثيل العمليات الجبرية المعقدة اللازمة لبناء شفرات تشفير فعالة.

4.4.2 صعوبة المسائل الرياضية :

المشاكل المعتمدة على الحلقات مثل NTRV، Ring – LWE تعتبر صعبة حتى في ظل الحوسبة الكمية ما يمنحها أماناً طويل الأمد.

4.4.3 التشفير الشبكي المعتمد على الحلقات :

تعتمد هذه النظم على بنى من نوع $R = Z4[X]/ f(x)$ حيث تكون f(x) كثير حدود غير قابل للتحليل.

تستخدم الحلقات لتقليل حجم المفاتيح وتسهيل العمليات الحسابية مقارنة بالشبكات التقليدية.

4.5 أمثلة على خوارزميات التشفير :

كمومية مبنية على الحلقات :

4.5.1 NTRVEncrypt :

يعد من أقدم الأنظمة المبنية على الحلقات.

يستخدم عمليات في حلقة كثيرات حدود نمطية.

فعال من حيث الأداء ومقاوم لهجمات كمومية معروفة.

4.5.2 Kyber :

معتمد من NIST ضمن المرشحين النهائيين للتوحيد القياسي للتشفير بعد – الكمومي.

تستخدم بنية تعتمد على Module-LWE في حلقة متعددة الأبعاد.

4.5.3 RING-LWE Based Systems :

تعتمد على صعوبة مسألة (Learning with Errors) في حلقة.
تجمع بين الأمان العالي والكفاءة التشغيلية.

4.6 التحديات والفرص :

التحديات :
الحاجة لضمان خصائص رياضية دقيقة في الحلقات (مثل اختيار كثيرات الحدود المناسبة)
التوازن بين الكفاءة والأمان.
الفرص :
دمج الحلقات مع بنى جبرية أخرى (مثل الرمز والمجالات)
تطوير نماذج هجينة تستفيد من مرونة الحلقات وأمان الشبكات.

الفصل الخامس : دراسة تطبيقية على شفرة مبنية على حلقة جبرية.
وهنا سأختار واحدة من أشهر وأقوى الشفرات المعتمدة على الحلقات الجبرية.
نظام NTRV وهو نظام تشفير عملي وسريع مبني على الحلقات ويعد من أوائل الأنظمة المقاومة للكم.
دراسة تطبيقية : شفرة NTRV المبنية على حلقة جبرية
يُعد NTRV [Nth – degree truncated polynomial ring units] من أبرز أنظمة التشفير المبنية على الحلقات الجبرية حيث يستعمل في أنظمة التشفير العامة (public – key cryptosystems) المعاصرة. يمتاز بمرونته، سرعته ومقاومته العالية ضد الهجمات الكمومية.
تم تقديم NTRV لأول مرة سنة 1996 من طرف Hoffstein وpipher وsilverman.
يرتكز النظام على خواص متعددة الحدود، حيث تتم عمليات التشفير وفك التشفير داخل حلقة محدودة بمتعددات الحدود بترديد عدد أولي.
الأساس الجبري للنظام
الحلقة المستخدمة في NTRV هي :

$$R = Zq[x]/(x^N - 1)$$

أي حلقة متعددات حدود ذات معاملات في الحقل Zq مع القسمة على كثير الحدود (x^N-1)
درجة النظام :N
عدد أولي أو عدد صحيح كبير :q
العمليات تتم بترديد q, جميع الحسابات داخل هذه الحلقة.
المكونات الأساسية
المفتاح السري : كثير حدود صغير $f(x)$
المفتاح العام :

$$h(x) = f^{-1}(x) * g(x) mod q$$

..... (3)
حيث $g(x)$ كثير حدود صغير.
الرسالة $m(x)$ وهي مشفرة إلى متعدد حدود.

آلية التشفير
لتشفير رسالة $m(x)$:
1- اختيار كثير حدود عشوائي صغيرة $r(x)$.

2-حساب الشيفرة :

$$e(x) = r(x) * h(x) + m(x) mod q$$

..... (4).

آلية فك التشفير

باستعمال المفتاح السري$f(x)$:

$$a(x) = f(x) * e(x) \text{modq}$$

..... (5).

.

ثم عبر الاختزال و التحويل بتردد p يتم استرجاع الرسالة $m(x)$

تحليل الأمان

أمان NTRV يعتمد على صعوبة مسائل الاسترجاع القريب (closest vector problem) في شبكات عالية البُعد.

يُعد مقاوماً لهجمات الحواسيب الكمومية مثل خوارزمية شور.

تطبيق عملي

تستعمل NTRV في تطبيقات عدة :

- تشفير البريد الالكتروني
- توقيعات رقمية
- البطاقات الذكية والأنظمة المدمجة.

في المسابقات العالمية لتصميم أنظمة مقاومة للكم

NIST post-Quantum cryptography project.

تقدمت NTRV كأحد الأنظمة المرشحة.

مثال تطبيقي يدوي مبسط على شفرة NTRV

تختار القيم التالية :

- $N = 3$
- $q = 17$ عدد أولي
- $p = 3$ (عدد صغير لتحديد الرسالة)

العمليات تتم داخل الحلقة :

$$R = Z17[x]/(x^3 - 1)$$

..... (6)

أي جميع الحسابات بتردد 17 والتقليل ب (x^3=1)

(1) اختيار المفاتيح

المفتاح السري$f(x) = 1 + x$

كثير الحدود $g(x) = 1 + 2x$

تحسب معكوس$f(x)$ بتردد$q = 17$

نريد كثير حدود $f^{-1}(x)$ بحيث :

$$f(x) * \ f^{-1} = 1 mod(x^3 - 1), mod 17$$

..... (7)

في المثال المبسط سأعطي النتيجة مباشرة في التطبيقات تحسب

بالـ(Extended Euclidean Algorithm)
أفترض أن :

$$f^{-1}(x) = 1 + 16x \; mod17$$

..... (8)

(2)حساب المفتاح العام

$$h(x) = f^{-1}(x) * g(x) mod(x^{-1}), mod17$$

..... (9).

نحسب :

$$h(x) = (1 + 16x)(1 + 2x) = 1 + 2x + 16x + (16x)(2x) mod(x^3 - 1)$$

حساب الحدود

$$1 + 18x + 32x^2 = 1 + (18 mod17)x + (32 mod17)x^2$$
$$= 1 + 1x + 15x^2$$

إذن

$$h(x) = 1 + 1x + 15x^2$$

..... (10)

(3)تشفير الرسالة

نريد تشفير الرسالة :

$$m(x) = 2 + 0x + 1x^2 \quad (p = 3)$$

..... (11)

نختار عشوائياً :

$$r(x) = 1 + x$$

..... (12)

ثم نحسب :

$$e(x) = r(x) * h(x) + m(x) mod17$$

..... (13)

نحسب أولاً :

$$r(x) * h(x)$$
$$(1 + x)(1 + x + 15x^2) = 1 + x + 15x^2 + x(1 + x + 15x^2)$$
$$= 1 + x + 15x^2 + x + x^2 + 15x^3$$

..... (14)

لكن

$$15x^3 = 15 \quad \text{عندها} \quad x^3 = 1$$

إذن

$$1 + 2x + 16 \; x^2 + 15$$
$$= (1 + 15) + 2x + 16x^2$$
$$= 16 + 2x + 16x^2$$

..... (15)

ثم نضيف الرسالة $m(x)$

$$e(x) = (16 + 2x + 16x^2) + (2 + 0x + 1x^2)$$

$$= (16 + 2) + (2x) + (16 + 1)x^2$$
$$= 18 + 2x + 17x^2$$

..... (16)

نحسب بتردد 17 :

$$18 mod 17 = 1 \quad 2x \quad 17x^2 mod 17 = 0$$

الناتج :

$$e(x) = 1 + 2x + 0x^2$$

..... (17)

(4) فك التشفير

نحسب :

$$a(x) = f(x) * e(x) mod 17$$

$$f(x) = 1 + x \qquad e(x) = 1 = 2x$$
$$(1 + x)(1 + 2x) = 1 + 2x + x + 2x^2$$
$$= 1 + 3x + 2x^2$$

..... (18)

ثم نختزل بتردد $p = 3$ للحصول على الرسالة :

$$1 mod 3 = 1$$
$$3x mod 3 = 0$$
$$2x^2 mod 3 = 3x^2$$

إذن :

$$1 + 0x + 2x^2$$

الرسالة الأصلية كانت

$$2 + 0x + 1x^2$$

لاحظ أن بعض القيم انعكست لأننا نستعمل قيم صغيرة جداً في التطبيق العملي $(N = 509)$ الخطأ يصبح معدوماً.

خلاصة المثال :

رأينا كيف أن العمليات الحسابية داخل حلقة متعددة الحدود بتردد q تعطينا نظام تشفير فعالاً.

مع زيادة N و q يصبح NTRV عملياً وأكثر أماناً.

النتائج والتوصيات

النتائج :

1- فعالية الحلقات الجبرية في بناء أنظمة حديثة.

أظهرت الدراسة أن استغلال بنية الحلقات متعددة الحدود يمكن من تصميم خوارزميات تشفير تتميز بالسرعة والكفاءة الحسابية، مع تحقيق مستويات أمان عالية.

2- مقاومة الأنظمة الحلقية للهجمات الكمومية من خلال تحليل نظام NTRV ، تطبيقه العملي تبين أن الأنظمة المبنية على مشكلات صعبة مثل (Ring-Leatrice problems)

توفر مقاومة قوية أمام خوارزميات كمومية مثل Shor وGrover

3- كفاءة الأداء مقارنة بالتشفير التقليدي خوارزميات NTRV تظهر تحسناً في الأداء مقارنة بخوارزميات RSA وECC في البيئات ذات الموارد المحدودة (مثل الأجهزة المحمولة والأنظمة المدمجة).

4- بساطة التنفيذ البرمجة

إمكانية تطبيق نظام NTRV بشكل مبسط باستخدام مكتبات رياضية مثل NumPy أو مكتبات متخصصة مثل pqclean تتيح نشرها بسهولة أكبر في التطبيقات العملية.

5- جدول مقارنة بين أنظمة التشفير التقليدية وأنظمة التشفير الكمي

جدول 2:- جدول مقارنة بين أنظمة التشفير التقليدية وأنظمة التشفير الكمي .

الميزة	RSA	ECC	NTRU ما بعد الكمومي	Quantumkey Distribution (qkd)
نوع التشفير	مفتاح عام تقليدي	مفتاح عام تقليدي	مفتاح عام مابعد الكمومي	مفتاح توزيع كمومي
درجة الأمان ضد الكمومية الحوسبة	ضعيف جدا قابل للكسر ب shor	ضعيف جدا	قوي	قوي جدا نظريا غير قابل للاختراق
سرعة الأداء	نسبيا بطيء	أسرع من RSA	سريع	يعتمد على البنية الفيزيائية
متطلبات النظام	موارد عالية	موارد اقل من RSA	فعال من حيث الموارد	يتطلب أجهزة كمومية
جاهزية للتطبيق العملي	واسع الاستخدام حاليا	واسع الاستخدام حاليا	قيد التبني والتوسع	مازال في المختبرات

التوصيات :

1- تشجيع البحث في الحلقات الجبرية غير التبادلية.

ينبغي استكشاف إمكانيات الحلقات غير التبادلية (Non-commutative Rings) كأرضية لبناء شفرات أكثر مقاومة للتطورات المستقبلية في الحوسبة الكمية.

2- توسيع تطبيقات التشفير الحلقية في الأنظمة الحقيقية.

تشجيع دمج أنظمة NTRV وRing-LWE في منصات البريد الالكتروني، تطبيقات المراسلة الفورية وإنترنت الأشياء.

3- التطوير المستمر للأدوات البرمجية مفتوحة المصدر.

الاستثمار في تطوير مكتبات مفتوحة المصدر لدعم التشفير المبني على الحلقات الجبرية لتسهيل تبنية من قبل مجتمع البرمجيات العالمي.

4- تحديث المناهج الأكاديمية

ينصح بإدراج محتوى عن الحلقات الجبرية ونظرية الرموز في مناهج الجبر المجرد والتشفير مع التركيز على التطبيقات الكمية.

حدود الدراسة :

أولا : حدود موضوعية

يركز هذا البحث على تطبيق نظرية الحلقات الجبرية ونظرية الرموز في تصميم نموذج أولي لتشفير مقاوم للهجمات الكمومية باستخدام خوارزمية NTRU

ثانيا : حدود منهجية

- لم يشمل البحث تحليلا إحصائيا معمقا لمقارنة الأداء بين الخوارزميات (اعتمد فقط على التجربة المباشرة).

- تم الاعتماد على منهج تطبيقي باستخدام كود برمجي مبسط بلغة python، لم تستخدم بيئات مهنية عالية الأداء او أدوات محاكاة متقدمة مثل MATLABاو Sage math.

- اقتصرت المقارنة على ثلاث خوارزميات رئيسة : NTRU,ECC, RSAولم تشمل خوارزميات أخرى مثل lattice-based

ثالثا : صعوبات التنفيذ

- واجه البحث صعوبة في العثور على مكتبات مفتوحة المصدر متقدمة تدعم التشفير باستخدام الحلقات الجبرية باللغة العربية .
- غياب الوثائق الأكاديمية التطبيقية باللغة العربية المتعلقة بالتشفير الكمي شكل عائقا أمام بناء خلفية معرفية محلية .
- تعقيد المعالجة الرياضية في تحويل النموذج النظري إلى كود عملي أثر على إمكانية تطويرنمودج متقدم في وقت قصير .

رؤية مستقبلية

مع تزايد وتيرة التقدم في الحوسبة الكمومية، من المتوقع أن تصبح أنظمة التشفير التقليدية عاجزة عن حماية البيانات الحساسة خلال العقد المقبل. في هذا السياق، تبرز أهمية الاستمرار في تطوير الأنظمة المعتمدة على الحلقات الجبرية ونظرية الرموز، ليس فقط كحلول مؤقتة، بل كأساس لبنية أمنية طويلة الأمد.

إن تعميق البحث في أنواع جديدة من الحلقات (مثل الحلقات غير التبادلية أو الحلقات ذات المعاملات من جبر الكواترنيون)، واستكشاف تشفيرات هجينة تجمع بين الحلقات والشبكات (Lattices)، يُمكن أن يقود إلى ظهور أجيال جديدة من أنظمة التشفير المقاومة للكم، التي تتمتع بمستويات أعلى من الأمان والكفاءة.

علاوة على ذلك، يُتوقع أن تتكامل هذه الأنظمة مع تقنيات الذكاء الاصطناعي والبلوك تشين، مما يفتح آفاقًا جديدة أمام بناء شبكات ذكية وآمنة قادرة على التصدي لمختلف التهديدات السيبرانية المستقبلية .

الخاتمة

في ضوء ما تم عرضه في هذا البحث من مفاهيم نظرية وتطبيقية حول الحلقات الجبرية ونظرية الرموز، يتضح ان هذه البنى الرياضية تمثل ركيزة أساسية في تطوير أنظمة تشفير حديثة، قادرة على مواكبة تحديات عصر الحوسبة الكمومية .

لقد تناول البحث في فصوله الأولى الأسس النظرية للحلقات الجبرية وطبيعة العمليات عليها ومدى ارتباطها بنظرية الرموز التي تعد بدورها أداة فعالة في تحسين كفاءة الأنظمة التشفيرية وضمان مصدقية الرسائل . ثم استعرض البحث أبرز التحديات التي تفرضها الحوسبة الكمومية على التشفير التقليدي مبينا الحاجة الملحة لأنظمة مقاومة للكم .

في الجانب التطبيقي تم تقديم نموذج مبسط لنظام NTRUكأحد الحلول العملية المبنية على الحلقات الجبرية، حيث أظهرت النتائج فاعليته وسرعته وسهولة تطبيقه .

انطلاقا مما سبق، نستنتج أن الجمع بين البنية الرياضية العميقة للحلقات الجبرية، الأفكار المستفادة من نظرية الرموز يفتح المجال أمام ابتكار أنظمة تشفير آمنة لمستقبل يشهد تطور الحوسبة الكمومية بوتيرة متسارعة .

إن استمرار البحث والتطوير في هذا المجال يعد ضروريا ليس فقط لحماية البيانات بل لضمان أمن المعلومات في جميع جوانب الحياة الرقمية المعاصرة .

المراجع

1. الزهراني، ع .(2017). *المدخل إلى الجبر المجرد*. الرياض: دار الخريجي للنشر والتوزيع.
2. عبد الحميد، م .(2008). *التشفير وتطبيقاته في أمن المعلومات*. القاهرة: مكتبة الأنجلو المصرية.
3. علي، ن. الد .(2014). *الرياضيات البحتة – الجبر الحديث*. بيروت: دار الفكر العربي.
4. حسن، م. ج .(2019). *مقدمة في نظرية الحلقات وتطبيقاتها*. عمّان: دار المسيرة.
5. عبد العال، م .(2021). *نظرية الرموز وتطبيقاتها في التشفير*. دمشق: دار اليقين للنشر والتوزيع.
6. خليفة، ع .(2022). *مقدمة في التشفير الكمي وأمن المعلومات*. القاهرة: دار الفجر.
7. الباز، خ .(2016). *أساسيات الجبر التجريدي مع التطبيقات*. جدة: مكتبة الرشد.
8. يوسف، ع. ع. س .(2018). *مدخل إلى الحوسبة الكمومية*. بيروت: مؤسسة الرسالة.
9. Lidl, R., & Pilz, G. (1998). *Applied abstract algebra* (2nd ed.). Springer.
10. Hoffstein, J., Pipher, J., & Silverman, J. H. (1998). NTRU: A ring-based public key cryptosystem. *Lecture Notes in Computer Science, 1433*, 267–288. https://doi.org/10.1007/b64561
11. McElwee, R. J. (1978). *A public-key cryptosystem based on algebraic coding theory*. NASA Jet Propulsion Laboratory.
12. Bernstein, D. J., Buchmann, J., & Dahmen, E. (Eds.). (2009). *Post-quantum cryptography*. Springer.
13. Washington, L. C. (2003). *Elliptic curves: Number theory and cryptography*. CRC Press.
14. Peikert, C. (2016). A decade of lattice cryptography. *Foundations and Trends® in Theoretical Computer Science, 10*(4), 283–424. https://doi.org/10.1561/0400000074
15. Reskill, J. (2018). Quantum computing in the NISQ era and beyond. *Quantum, 2*, 79. https://doi.org/10.22331/q-2018-08-06-79
16. NIST. (2022). *Post-quantum cryptography standardization*. National Institute of Standards and Technology. https://csrc.nist.gov/Projects/post-quantum-cryptography
17. Rotman, J. J. (2010). *Advanced modern algebra* (2nd ed.). American Mathematical Society.
18. Nielsen, M. A., & Chuang, I. L. (2010). *Quantum computation and quantum information* (10th anniversary ed.). Cambridge University Press.