دراسة كفاءة أنظمة التّشفير $MDNA، ELQTR، ELTRU$

مريم يوسف المصطفى–طالبة ماجستير في كليّة العلوم–قسم الرياضيات–جامعة حمص.

أ.م.د. باسل حمدو العرنوس–كليّة العلوم–قسم الرياضيات–جامعة حمص.

أ.د. حسن راشد ياسين– كليّة التربية–قسم الرياضيات–جامعة القادسية–العراق.

ملخّص البحث

تقدم هذه الورقة دراسة تحليلية مقارنة لثلاثة أنظمة تشفير حديثة ومطورة لنظام $NTRU$، وهي:

- $ELTRU$ القائم على الجبر الحادي عشر الجديد.
- $ELQTR$ الذي يدمج الجبر الحادي عشر مع معاملات من الجبر الرباعي.
- $MDNA$ الذي يدمج الجبر الحادي عشر مع تشفير الحمض النووي DNA.

تركز المقارنة لهذه الأنظمة بناءً على معيارين رئيسيين:

- قوة الأمان ممثلة بحجم فضاء العينة للمفتاح الخاص وللرسالة
- الوقت المستغرق للتنفيذ (العمليات الحسابية لجميع مراحل كل طريقة).

الكلمات المفتاحيّة:

حلقة كثيرات الحدود المقطوعة، الجبر الحادي عشر، الحمض النووي منقوص الأكسجين، فضاء العينة للرسالة، فضاء العينة للمفتاح، نظام التشفير $ELTRU$، نظام التشفير $ELQTR$ ، نظام التشفير $MDNA$، الجبر الرباعي، الجبر الثماني.

" Evaluating the Efficiency of ELTRU, ELQTR, and MDNA Encryption Systems"

Mariam Yosef Al-mustafa– Faculty of Science – Department of mathematics –Homs university.

Dr. **Basel Hamdo Alarnous** – Faculty of Science – Department of mathematics– Homs university.

P.Dr. **Hassan Rashed Yassein** – Department of mathematics– College of Education– University of Al-Qadisiyah– Iraq.

Abstract

This paper presents a comprehensive comparative analytical study of three modern and enhanced encryption systems developed for the NTRU cryptosystem، namely:

- **ELTRU**, which is based on a new eleventh algebra.
- **ELQTR**, which integrates eleventh algebra with quaternion algebra Coefficients.
- **MDNA**, which integrates eleventh algebra with DNA-based encryption.

The comparison of these systems is conducted based on two main criteria:

- **Security strength**, represented by the key space size for the private key and the message.
- **Execution time**, measured by the computational operations required for all stages of each method.

Key Words:

Truncated polynomial ring, MAL-Eleven algebra, DNA, Space security of key, Space security of Message, $NTRU$ Cryptosystem،

ELTRU Cryptosystem, *ELQTR* Cryptosystem, *MDNA* Cryptosystem, Quaternion algebra, Octonion algebra.

مقارنة بين أنظمة التّشفير $ELTRU$ و$ELQTR$ و$MDNA$

1. مقدّمة

مع تطور التكنولوجيا أصبح التشفير علماً لا غنى عنه، فهو يعمل على تغيير شكل البيانات بمختلف أنواعها المالية والمصرفية والعسكرية والأمنية والسياسية والاقتصادية بشكل يصعب فهمها حتى وإن تمّ الاطلاع عليها من قبل أشخاص غير مخوّلين لذلك.

ويعتمد التشفير على الرياضيات وخوارزميات صعبة التشكيل، وقد طوّر العلماء العديد من أنظمة تشفير المفتاح العام منذ تقديم طريقة (Diffie Hellman) في عام 1976 [1].

ومن بين هذه التطورات برز نظام التّشفير $NTRU$ [2] لتميّزه بأمان عالٍ وسرعة تنفيذ عالية وحجم مفاتيح صغير، ويعتمد هذا النظام على حلقة كثيرات الحدود المقطوعة.

وفي السنوات الأخيرة، ظهر نوع مبتكر من التّشفير يُعرف باسم تشفير الحمض النووي مستوحى من البنية الفريدة للحمض النووي، تتميز هذه الأنظمة بقدرة كبيرة على خزن المعلومات وسرعة تنفيذ عالية.

وقد قدّم العلماء العديد من التحسينات لنظام $NTRU$ وللأنظمة القائمة على الحمض النووي وسنتحدث عن البعض منها:

1. في العام 2009 قدّم $Malekian$ وآخرون ببناء نظام تشفير يعتمد على الجبر الرباعي أطلقوا عليه اسم $QTRU$ [3]، وتوصّلوا إلى أنّ $QTRU$ أكثر مقاومة لبعض الهجمات من $NTRU$.
2. وفي العام 2010 اقترح $Malekian$ وآخرون [4] نظام تشفير مطور لـ $NTRU$ يعتمد على الجبر الثماني يُسمى $OTRU$.
3. في العام 2016 قدّم $Yassein$ وآخرون[5] جبر جديد يُدعى الجبر السادس عشر لإنشاء نظام التشفير $HXDTRU$.

4. في العام 2019 قدّم $Almahdi$ وآخرون [6] تقنية تشفير غير متناظر تعتمد على الحمض النووي لتشفير وفك تشفير النصوص.
5. في العام 2025 قدّم $Albakaa$ وآخرون [7] نظام التشفير $FDNA$ الذي يعتمد على الحمض النووي وكثيرات الحدود ويوفر هذا النظام مستوى عالٍ من الأمان.
6. في العام 2025 قدّم $Yassein$ و آخرون [8] نظام التشفير $PDNA$ يعتمد على الحمض النووي وكثيرات الحدود ويوفر هذا النظام مستوى أمان عالٍ جداً.
7. وفي العام 2025 قدّمت $Almustafa$ وآخرون [9] جبر جديد يُدعى الجبر الحادي عشر M_{ae} لإنشاء نظام التشفير $ELTRU$ وهو نظام تشفير مطور لـ $NTRU$ ويوفر هذا النظام مستوى عالٍ من الأمان.
8. وفي العام 2025 قدّمت $Almustafa$ و $Alarnous$ وآخرون [10] نظام التشفير $ELQTR$ ويعتمد على الجبر الحادي عشر بمعاملات من الجبر الرباعي مما يوفر مستوى أمان عالٍ جداً.
9. وفي العام 2026 قدمت $Almustafa$ و $Yassein$وآخرون [11] نظام التشفير $MDNA$ وهو نظام تشفير يعتمد على الجبر الحادي عشر والحمض النووي معاً يتميز هذا النظام بسرعة عالية ومستوى أمان عالٍ جداً.

2. مشكلة البحث

في ظل التزايد المستمر في حجم تبادل البيانات عبر الشبكات الرقمية وارتفاع مخاطر الاختراق والتلاعب بالمعلومات، برزت الحاجة إلى تطوير أنظمة تشفير أكثر أماناً وكفاءة، ومن بين الأنظمة المقترحة ظهرت أنظمة التشفير $ELTRU$ و$ELQTR$ و$MDNA$.

تكمن مشكلة البحث في دراسة وتحليل الفروقات بين هذه الأنظمة من حيث مستوى الأمان ووقت التنفيذ حتى يتمكن المستخدم من اختيار الطريقة المناسبة له حسب حاجته.

3. هدف البحث

يهدف هذا البحث إلى إجراء دراسة تحليلية مقارنة بين أنظمة التشفير $ELTRU$ و$ELQTR$ و$MDNA$ من أجل تقييم مستوى الأمان والكفاءة الحسابية لكل نظام ويهدف تقديم بعض الاقتراحات لتطوير هذه الأنظمة.

4. المناقشة والنتائج

4 – 1: التعاريف الأساسيّة

نقدّم بدايةً تعريفاً لكل من أنظمة التّشفير $ELTRU$و$ELQTR$ و$MDNA$

تعريف 1:[9]

نظام التّشفير $ELTRU$: هو نظام مُحسن لنظام $NTRU$ يعتمد على جبر جديد يُدعى الجبر الحادي عشر وعلى حلقة كثيرات الحدود المقطوعة.

جرى مقارنة هذا النّظام مع $NTRU$ وبعض تحسيناته ($QTRU$،$OTRU$) ووُجِد أنّه يتمتع بمستوى أمان عالٍ جداً بالنسبة لفضاء العينة للمفتاح وللرسالة مقارنة بالأنظمة السابقة كما أنّه أسرع من $QTRU$ و$OTRU$ وأبطأ من $NTRU$ ولكن يمكن التغلب على مشكلة السرعة بتخفيض درجة كثيرات الحدود.

تعريف 2:[10]

نظام التّشفير $ELQTR$:هو نظام تشفير مُحسن لنظام $NTRU$ يعتمد على الجبر الحادي عشر بمعاملات من الجبر الرباعي وعلى حلقة كثيرات الحدود المقطوعة.

جرى مقارنة هذا النّظام مع $NTRU$ وبعض تحسيناته ($QTRU$،$OTRU$) ووُجِد أنّه يتمتع بمستوى أمان عالٍ جداً بالنسبة لفضاء العينة للمفتاح وللرسالة مقارنة بالأنظمة السابقة ولكنه أبطأ من $QTRU$ و$OTRU$ و $NTRU$ ولكن يمكن التغلب على مشكلة السرعة بتخفيض درجة كثيرات الحدود.

تعريف 3:[11]

نظام التّشفير $MDNA$: وهو نظام تشفير مُحسن لنظام $NTRU$ يعتمد على الجبر الحادي عشر والحمض النووي وحلقة كثيرات الحدود المقطوعة. هذا الدمج أعطى نظاماً قوياً يتمتع بدرجة أمان عالية من خلال الطبيعية العشوائية للحمض النووي.

تم مقارنته بـ أنظمة تشفير مشابهة له وهي نظام التشفير $FDNA$ [7] ونظام التشفير $PDNA$ [8] ووُجِد أنّه يتفوق عليهما من حيث مستوى الأمان ولكنّه أبطأ منهما ولكن يمكننا التغلب على مشكلة السرعة بتخفيض درجة كثيرات الحدود.

والآن سنقوم بدراسة الفرق بين هذه الأنظمة من حيث مستوى الأمان ووقت التنفيذ.

4 – 2: المقارنة من حيث مستوى الأمان

من المعايير الرئيسية في أنظمة التشفير هو مستوى الأمان فكلّما كان مستوى الأمان عالٍ كلّما كانت هذه الطريقة مطلوبة في سوق العمل.

يمكن للمخترق الذي يعرّف المفتاح العام أن يسلك أحد الطريقين: إمّا أن يبحث حتى يحصل على المفاتيح الخاصة المستخدمة في مرحلة توليد المفتاح ويكمل مرحلة فك التشفير فيحصل على الرسالة الأصلية وهذا ما نطلق عليه فضاء العينة للمفتاح، أو أن يبحث في المفتاح الخاص المُستَخدم في مرحلة التشفير ومن خلاله يحصل على الرسالة الأصلية بدون الرجوع إلى باقي مراحل النظام وهذا ما نسمّيه فضاء العيّنة للرسالة.

4 – 2 – 1: مستوى أمان المفاتيح الخاصّة

جرى إيجاد فضاء العينة للمفتاح (مستوى أمان المفاتيح الخاصة)، لكل نظام من الأنظمة المدروسة في [9 – 10 – 11]

الجدول(1) يبين مقارنة من حيث مستوى أمان المفتاح الخاص للأنظمة $ELTRU$ و $ELQTR$ و $MDNA$.

الجدول (1): مستوى أمان المفتاح للأنظمة$MDNA$،$ELQTR$،$ELTRU$.

نظام التشفير	فضاء العينة للمفتاح
$ELTRU$	$\left(\frac{N!}{(d_g!)^2(N-2d_g)!}\right)^{11}$
$ELQTR$	$\left(\frac{N!}{(d_g!)^2(N-2d_g)!}\right)^{44}\left(\frac{N!}{(d_S!)^2(N-2d_S)!}\right)^{44}$
$MDNA$	$4^n\left(\frac{N!}{d_g!\,(d_g-1)!\,(N-2d_g+1)!}\right)^{11}$

نلاحظ من الجدول (1) أنَّ نظام التّشفير $ELQTR$ أعلى أماناً بالنسبة للمفتاح من نظام التّشفير $ELTRU$ ونظام التشفير $MDNA$ أعلى أماناً من نظام التّشفير $ELTRU$.

بينما بالنسبة للأنظمة $ELQTR$ و $MDNA$ بفرض أنَّ:

$$\frac{N!}{(d_g!)^2(N-2d_g)!}=\frac{N!}{(d_S!)^2(N-2d_S)!}=$$
$$=\frac{N!}{d_g!\,(d_g-1)!\,(N-2d_g+1)!}=x$$

فيكون فضاء العينة للمفتاح لـ $ELQTR$ هو x^{88} وفضاء العينة للمفتاح لـ $MDNA$ هو $4^n x^{11}$ ، لنناقش الحالات الآتية:

a) إذا كان $n > \frac{xlog(77)}{log(4)}$ فإنَّ نظام التّشفير $MDNA$ هو أعلى أماناً بالنسبة للمفتاح من نظام التّشفير $ELQTR$.

b) إذا كان $n < \frac{xlog(77)}{log(4)}$ فإنَّ مستوى أمان نظام التّشفير $ELQTR$ أعلى أماناً بالنسبة للمفتاح من مستوى أمان نظام التّشفير $MDNA$.

c) إذا كان $n = \frac{xlog(77)}{log(4)}$ فإنَّ مستوى أمان المفتاح لنظام التّشفير $MDNA$ يساوي مستوى أمان نظام التّشفير $ELQTR$.

هنا لا يمكننا القول بالمطلق أنَّ أحدهما أعلى أماناً بالنسبة للمفتاح من الأخر، حيث يمكن التحكّم في ذلك حسب الحاجة، وهذه نقطة إيجابية في عملنا وتخدمنا في الجانب المادي عند استخدام هذه الأنظمة، فالتكلفة أيضاً هي أحد المعايير التي تحدد مقدار كفاءة أنظمة التشفير.

4 − 2 − 2: مستوى أمان الرّسالة

نجري فيما يأتي مقارنة من حيث فضاء العينة للرسالة (مستوى أمان الرسالة).

الجدول(2) يبين مقارنة بين أنظمة التشفير $ELTRU$ و$ELQTR$ و$MDNA$ من حيث أمان الرسالة.

الجدول (2): مستوى أمان الرسالة للأنظمة$MDNA$،$ELQTR$،$ELTRU$

نظام التشفير	فضاء العينة للرسالة
$ELTRU$	$\left(\frac{N!}{(d_\varphi!)^2(N-2d_\varphi)!}\right)^{11}$
$ELQTR$	$\left(\frac{N!}{(d_\varphi!)^2(N-2d_\varphi)!}\right)^{44}\left(\frac{N!}{(d_\psi!)^2(N-2d_\psi)!}\right)^{44}$

$MDNA$	لا يوجد

من الجدول السابق نلاحظ أن نظام التشفير $MDNA$ لا يوجد به فضاء عينة للرسالة أي أنّ المخترق ليس أمامه الّا طريق واحد فقط، وهذه ميزة في هذا النظام ومنه نجد أن $MDNA$ أعلى أماناً من $ELTRU$ و $ELQTR$ بالنسبة للرسالة.

بينما بالنسبة لـ $ELTRU$ و $ELQTR$ نلاحظ أن $ELQTR$ أعلى أماناً من $ELTRU$ بالنسبة للرسالة.

والأشكال (1) و (2) و (3) و (4) تبيّن المقارنة بين الأنظمة $ELTRU$ و $ELQTR$ و $MDNA$ من حيث مستوى أمان المفتاح والرسالة.

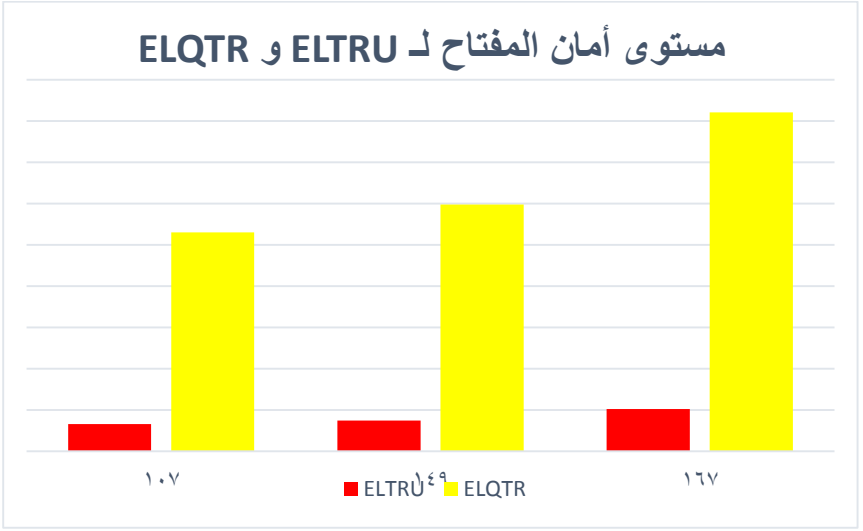
وذلك بتعويض القيم الواردة في الجدول(3) في الجداول (1) و (2).

الجدول(3): بعض القيم للعوامل d_φ و d_g و N.

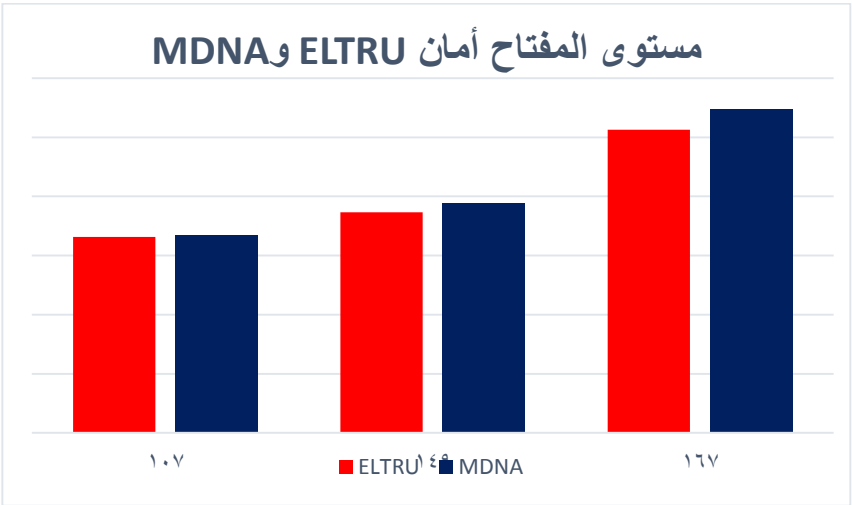
N	d_g	d_φ
107	12	5
149	12	10
167	18	18

أما بالنسبة لمستوى الأمان لـ $ELTRU$ و $MDNA$ أخذنا الحالات الثلاث لـ n فهي التي تعطي فرقاً بينهما (الشكل (3)).

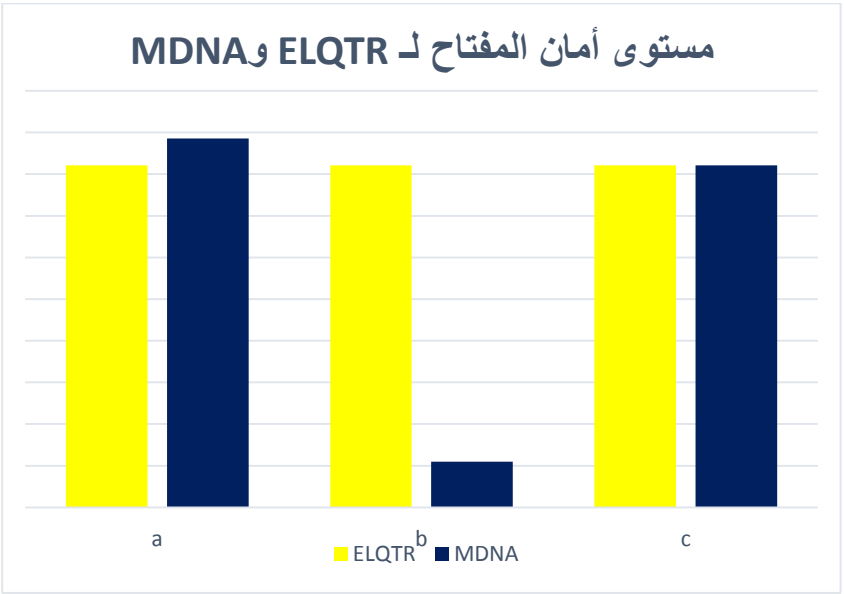
الشكل(1): مقارنة بين $ELTRU$ و $ELQTR$ من حيث مستوى أمان المفتاح.



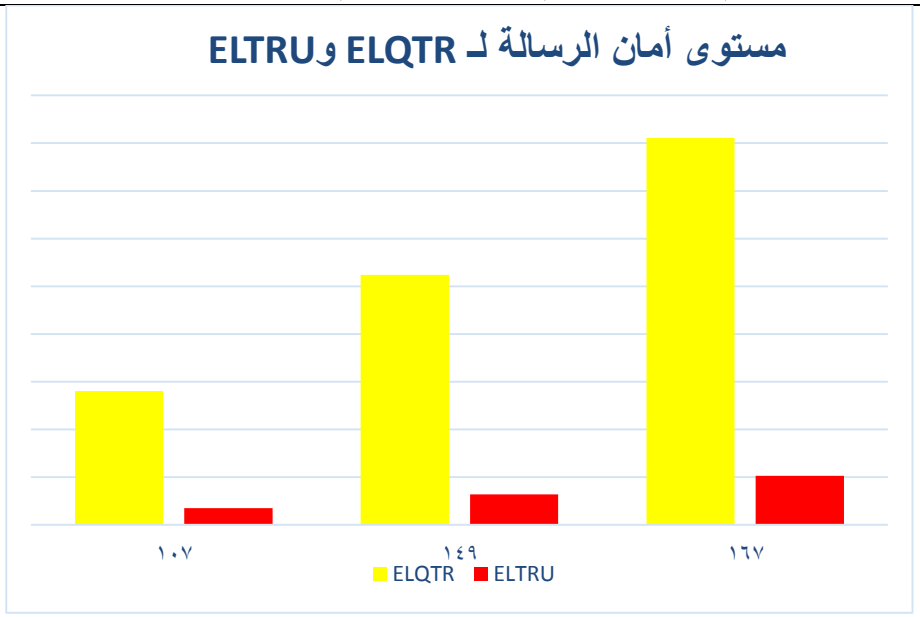
الشكل (2): مقارنة بين $ELTRU$ و $MDNA$ من حيث مستوى أمان المفتاح



الشكل(3): مقارنة بين $ELQTR$ و $MDNA$ من حيث مستوى أمان المفتاح.



الشكل(1.4): مقارنة بين $ELTRU$ و $ELQTR$ من حيث مستوى أمان الرسالة.



4 – 3: المقارنة من حيث وقت التنفيذ:

إلى جانب مستوى الأمان يعتبر وقت تنفيذ أنظمة التشفير من الأمور الهامة جداً عند اختيار نظام تشفير مناسب والجدول (4) يبين مقارنة بين أنظمة التشفير $ELTRU$ و $ELQTR$ و $MDNA$.

الجدول (4): مقارنة من حيث وقت التنفيذ للأنظمة $MDNA$،$ELQTR$،$ELTRU$.

نظام التشفير	$ELTRU$	$ELQTR$	$MDNA$
وقت التنفيذ	$44t_0 + 22t_1$	$3344t_0 + 176t_1$	$44t_0 + 2t_2$

حيث إنَّ t_0 تعبر عن وقت تنفيذ عمليات الضرب و t_1 تعبر عن وقت تنفيذ عمليات الجمع و t_2 تعبر عن وقت تنفيذ العمليات على الكودونات.

مما سبق نجد أنَّ نظام التّشفير $MDNA$ يتمتع بسرعة عالية ومن ثم يأتي نظام $ELTRU$ ومن ثم $ELQTR$ والشكل (5) يبين مقارنة بين أنظمة التشفير $ELTRU$ و$ELQTR$ و $MDNA$ من حيث وقت التنفيذ.

الشكل(1.5): مقارنة بين $ELTRU$ و$ELQTR$ و $MDNA$ من حيث سرعة التنفيذ.

يجدر التنويه إلى أنّه، على الرغم من وجود فروق واضحة بين الأنظمة من حيث زمن التّنفيذ، فإنَّ هذه الفروق تظلّ محدودة وتقتصر على أجزاءٍ من الثّانية.

5. نتائج البحث الرئيسة

لقد نجح هذا البحث في تحقيق سلسلة من الأهداف المترابطة التي تشكل معاً رؤية جديدة لأنظمة التشفير:

1. من حيث مستوى الأمان:

أولاً: أمان المفتاح الخاص:

تشير نتائج المقارنة إلى أن نظام $ETQTR$ يتمتع بمستوى أمان أعلى النسبة للمفتاح من نظام تشفير $ELTRU$.

كما يتبين أن نظام $MDNA$ يوفر درجة أمان أعلى من $ELTRU$ في هذا الجانب.

أما عند مقارنة $MDNA$مع $ELQTR$ فإن الأمان نسبي يعتمد بشكل أساسي القيم المختارة للمعلمات المستخدمة (خاصةً n في $MDNA$).

وبناءً على ذلك، يمكن لأيّ من النظامين تحقيق مستوى أمان أعلى من الآخر، الأمر الذي يمنح المستخدم مرونة إضافية في اختيار النظام بما يتناسب مع متطلبات الأمان.

ثانياً: أمان الرسالة:

يتمتع $MDNA$ بميزة كبيرة، حيث لا يوجد فضاء عينة للرسالة يمكن للمهاجم استغلاله، مما يضطره لمهاجمة المفتاح فقط. ونتيجة لذلك يُعد $MDNA$ النظام الأعلى أماناً من حيث حماية الرسالة.

وبالمقارنة بين نظامي التشفير $ELTRU$ و$ELQTR$ يتضح أن $ELQTR$ يحقق مستوى أمان أعلى فيما يتعلق بالرسالة.

2.من حيث وقت التنفيذ:

أظهرت نتائج المقارنة أن ترتيب الأنظمة من حيث سرعة التنفيذ، هو كما يلي:

- $MDNA$ (الأسرع)
- $ELTRU$
- $ELQTR$ (الأبطأ)

يُشار إلى أن الفروق في سرعة التنفيذ بين هذه الأنظمة هي في حدود أجزاء من الثانية، ويمكن تحسين الأنظمة الأبطأ $(ELTRU, ELQTR)$ عن طريق تخفيض درجة كثيرات الحدود المستخدمة.

والجدول (5) يبين النتائج التي توصلنا إليها:

الجدول (5): يبين النتائج التي توصلنا إليها.

تطبيقات النظام	العيب النسبي	الميزة الرئيسية	النظام
تشفير البيانات التي تحتاج توازناً بين السرعة والأمان	مستوى أمان أقل مقارنة بالأنظمة الأخرى	توازن جيد بين الأمان والسرعة، أسرع من $ELQTR$	$ELTRU$
تشفير البيانات الحساسة جداً حيث يكون الأمان أولوية قصوى على حساب السرعة.	الأبطأ من حيث وقت التنفيذ.	أعلى مستوى أمان بالنسبة للمفتاح والرسالة من $ELTRU$	$ELQTR$
تشفير البيانات التي تتطلب أعلى مستويات الأمان مع وقت تنفيذ أقل، خاصة عند التعامل مع بيانات حساسة للغاية.	زيادة العمليات الحسابية بسبب دمج كثيرات الحدود مع الـ DNA	أعلى أمان وسرعة تنفيذ عالية (الأسرع)، ومرونة في التحكم بأمان المفتاح الخاص.	$MDNA$

6. المقترحات والتوصيات

يقترح هذا العمل عدة مسارات بحثية واعدة:

- تحسين بعض أنظمة تشفير المفتاح العام باستخدام الجبر الحادي عشر من أجل زيادة مستوى الأمان.
- يمكن استخدام جبر مختلف على نفس البنية الرياضية في $MDNA$ لإنشاء نظام تشفير يكون أكثر أماناً.

7. المراجع

1. W. Diffie and M. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644–654, Nov. **1976**.
2. J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A ring-based public key cryptosystem," in Proceedings of the Third International Symposium on Algorithmic Number Theory (ANTS-III), Portland, OR, USA, Jun. **1998**, vol. 1423, pp. 267–288: Springer Berlin Heidelberg.
3. E. Malekian, A. Zakerolhosseini, and A. Mashatan, "QTRU: A lattice attack resistant version of NTRU PKCS based on quaternion algebra," The ISC International Journal of Information Security, vol. 3, no. 1, pp. 29–42, **2011**.
4. E. Malekian and A. Zakerolhosseini, "OTRU: A non-associative and high speed public key cryptosystem," in Proceedings of the 15th CSI International Symposium on Computer Architecture and Digital Systems (CADS), Tehran, Iran, **2010**, pp. 83–90.
5. H. R. Yassein and N. M. G. Al-Saidi, "HXDTRU cryptosystem based on hexadecnion algebra," in Proceedings of the 6th International Cryptology and Information Security Conference (CRYPTOLOGY), Kota Kinabalu, Malaysia, **2016**, pp. 1–10.
6. H. Al-Mahdi, M. Alruily, O. R. Shahin, and K. Alkhaldi, "Design and analysis of DNA encryption and decryption technique based on asymmetric cryptography system," International Journal of Advanced Computer Science and Applications, vol. 10, no. 2, pp. 499–506, **2019**.
7. F. H. Albakaa and H. R. Yassein, "A new encryption scheme based on DNA and polynomials with more security," International Journal of Mathematics and Computer Science, vol. 20, no. 1, pp. 383–386, **2025**.
8. F. H. Albakaa and H. R. Yassein, "A new method of encryption based on octonion algebra and DNA," AIP Conference Proceedings, **2025**.

9. M. Y. Almustafa, B. H. Alarnous, and H. R. Yassein, "ELTRU: Development of NTRU via newly eleventh-dimensional algebra," Boletim da Sociedade Paranaense de Matemática, vol. 43,no.3s, pp. 1–7, **2025**.
10. M. Y. Almustafa, B. H. Alarnous, and H. R. Yassein, "ELQTR: More secure encryption system based on MAL-Eleven algebra with quaternion coefficients," Boletim da Sociedade Paranaense de Matemática, vol. 43, no. 3, pp. 1–5, **2025**.
11. M. Y. Almustafa, B. H. Alarnous, and H. R. Yassein, "DNA and MAL-eleven algebra to design an efficient encryption cryptosystem," Boletim da Sociedade Paranaense de Matemática, vol. 44, pp. 1–4, **2026**