African Journal of Advanced Pure and Applied Sciences (AJAPAS)
Online ISSN: 2957-644X
Volume 5, Issue 3, 2026
Page No: 48-63
Website: https://aaasjournals.com/index.php/ajapas/index
ISI 2025: 1.126 SJIFactor 2024: 6.752 معامل التأثير العربي: 1.62

Improving Coding Performance Using Numerical Methods and an Applied Study on Elliptical Curves

Arij A. Awin [1 *], Aml A. Altirban [2], Sabrina A. Belhabla [3]
[1,2,3] Department of Mathematics, Faculty of Science, Tripoli University, Tripoli, Libya

تحسين أداء التشفير باستخدام الطرق العددية ودراسة تطبيقية على المنحنيات البيضاوية

أريج علي عوين [1*]، أمل عبد الله الطربان [2] ، صبرينة امحمد بلحبلة [3]
[1،2،3] قسم الرياضيات، كلية العلوم، جامعة طرابلس، طرابلس، ليبيا

*Corresponding author: ar.awin@out.edu.ly

Received: April 15, 2026	Accepted: June 26, 2026	Published: July 12, 2026

Abstract:
Modern digital infrastructures, including smart cities and the Internet of Things (IoT), increasingly require secure and efficient cryptographic mechanisms to ensure data confidentiality and privacy. Elliptic Curve Cryptography (ECC) has become one of the most widely utilized encryption schemes because it provides strong security with relatively small key sizes compared to traditional algorithms such as RSA. However, the practical deployment of ECC encounters several numerical and computational challenges related to efficiency and precision, especially when operating over large finite fields or within resource-constrained devices. This research addresses these challenges by integrating advanced numerical methods to improve the performance of ECC algorithms. The study examines the core arithmetic operations in ECC—specifically point addition and point multiplication—and identifies critical computational stages that can benefit from numerical optimization. A set of numerical techniques is reviewed and applied, including the Newton–Raphson method to accelerate modular inverse calculations, numerical integration methods such as the trapezoidal rule and Simpson's rule to approximate nonlinear elliptic-curve functions, and fast multiplication algorithms.
To validate the proposed approach, an applied experimental study was conducted using MATLAB. Experimental codes were developed to implement ECC algorithms enhanced with the selected numerical methods. Performance evaluation was based on key metrics such as execution time, computational accuracy, and numerical error magnitude. The study also explores the potential use of artificial intelligence techniques, including machine learning algorithms, to optimize initial parameter selection and accelerate convergence in iterative processes.
The results demonstrate clear improvements in execution time and significant reductions in numerical error, confirming the effectiveness of numerical methods in enhancing ECC performance for modern resource-limited systems.

Keywords: Elliptic Curve Cryptography; Newton-Raphson Method; Numerical Integration; Machine learning Optimization.

الملخص
شهدت الأنظمة الرقمية الحديثة، مثل المدن الذكية وإنترنت الأشياء طلبًا متزايدًا على تقنيات تشفير آمنة وفعّالة قادرة على حماية البيانات وضمان الخصوصية، وتُعد خوارزميات التشفير بالمنحنيات البيضاوية (Elliptic Curve Cryptography – ECC) من أكثر تقنيات التشفير اعتمادًا نظرًا لقدرتها على توفير مستوى عالٍ من الأمان باستخدام مفاتيح صغيرة الحجم مقارنة بخوارزميات تقليدية مثل RSA ومع ذلك، تواجه خوارزميات ECC تحديات عددية وحسابية تتعلق بالكفاءة والدقة خاصة عند العمل على الحقول الرياضية الكبيرة أو عند تطبيقها في الأجهزة ذات الموارد المحدودة. يهدف هذا البحث إلى معالجة هذه التحديات من خلال دمج الطرق العددية المتقدمة لتحسين أداء خوارزميات ECC. تم التركيز على تحليل العمليات الحسابية الأساسية في ECC ، مثل جمع النقاط ومضاعفتها، وتحديد المراحل الحرجة التي يمكن تحسينها عدديًا. كما تم استعراض وتطبيق مجموعة من الطرق العددية، من بينها طريقة نيوتن–رافسون لتسريع حساب

المعكوس المعياري، وطرق التكامل العددي مثل طريقة شبه المنحرف وطريقة سمبسون لتقدير بعض الدوال غير الخطية المرتبطة بالمنحنيات البيضاوية بالإضافة إلى خوارزميات الضرب السريع.
ولإثبات فعالية المنهجية المقترحة، أُجريت دراسة تطبيقية باستخدام برنامجMATLAB حيث تم تطوير أكواد تجريبية لتنفيذ خوارزميات ECC مع دمج الطرق العددية المختلفة، وتم تقييم الأداء بالاعتماد على معايير أساسية شملت زمن التنفيذ والدقة الحسابية وحجم الخطأ العددي، كما تم استكشاف إمكانية دمج تقنيات الذكاء الاصطناعي مثل خوارزميات التعلم الآلي لتحسين اختيار القيم الابتدائية وتسريع التقارب في العمليات التكرارية، أظهرت النتائج تحسنًا ملحوظًا في زمن التنفيذ وانخفاضًا في الخطأ العددي مقارنة بالطرق التقليدية مما يؤكد دور الطرق العددية في تعزيز كفاءة ECC وجعلها أكثر ملاءمة للتطبيقات العملية الحديثة.

الكلمات المفتاحية: المنحنى البيضاوي، التشفير، نيوتن-رافسون، الخطأ العددي، التعلم الآلي.

مقدمة

شهد مجال التشفير تطورا متسارعا خلال العقود الأخيرة مدفوعا بالتحول الرقمي المتزايد والحاجة المتنامية إلى حماية البيانات في الأنظمة الرقمية الحديثة مثل المدن الذكية إنترنت الأشياء والاتصالات الآمنة، وقد أدى هذا التطور إلى البحث عن خوارزميات تشفير توفر مستويات عالية من الأمان مع كفاءة حسابية مناسبة للبيئات ذات الموارد المحدودة.
يعد التشفير بالمنحنيات البيضاوية (Elliptic Curve Cryptography (ECC)) من أبرز تقنيات التشفير بالمفتاح العام (فريد بايبر واخرون، 2016) التي أثبتت فاعليتها في هذا السياق نظرا لقدرته على تحقيق مستوى أمان مكافئ للخوارزميات التقليدية باستخدام أطوال مفاتيح أصغر نسبيا مما ينعكس إيجابا على تقليل الحمل الحسابي واستهلاك الذاكرة والطاقة، ويعتمد ECC بصورة أساسية على العمليات الحسابية على نقاط المنحنيات البيضاوية ولا سيما عمليتي جمع النقاط ومضاعفة النقطة (Ian Blake, et al 1999)، اللتين تمثلان جوهر عمليات التشفير وفك التشفير وتوليد المفاتيح.
وعلى الرغم من المزايا الأمنية التي يوفرها ECC، فإن تطبيقه العملي يواجه عددا من التحديات الحسابية من بينها تعقيد العمليات الرياضية، والدقة العددية، واستقرار الخوارزميات، إضافة إلى الزمن اللازم لتنفيذ العمليات خاصة عند التعامل مع أحجام وبيانات كبيرة وأنظمة ذات قدرات محدودة. وهنا يبرز دور الطرق العددية ($Numerical\ Methods$) (علي عوين،2010) كأدوات فعّالة لتحسين كفاءة هذه العمليات من خلال تقليل التعقيد الحسابي وتسريع الأداء دون التأثير على مستوى الأمان المطلوب (Andreas Enge, 2012).
يهدف هذا البحث إلى دراسة أثر استخدام الطرق العددية على تحسين أداء خوارزميات التشفير بالمنحنيات البيضاوية من خلال الجمع بين التحليل النظري والتطبيق العملي. حيث يتم في الجزء الأول استعراض الخلفية النظرية حول للتشفير العددي والمنحنيات البيضاوية، مع التركيز على العمليات الحسابية الأساسية مثل جمع النقطتين ومضاعفة النقطة. أما الجزء التطبيقي فيتناول دراسة باستخدام برنامج MATLAB لتحليل أداء الطرق العددية عند تطبيقها على خوارزميات ECC من خلال إجراء محاكاة عددية وقياس زمن التنفيذ ومقارنة النتائج من حيث الكفاءة والتحسين في الأداء.
وتسعى هذه الدراسة إلى إبراز الدور المحوري للطرق العددية في تعزيز كفاءة وأداء أنظمة التشفير الحديثة وتحقيق توازن بين الأمان العالي والكفاءة الحسابية بما يدعم هذه الدراسة تطوير تطبيقات عملية تعتمد على ECC في مجالات تقنية متنوعة.

1. المنحنيات البيضاوية

تعريف 1.1

تعد المنحنيات البيضاوية "$Elliptic\ Curves$"من المواضيع البارزة في الرياضيات الحديثة والتطبيقات العملية، خاصة في مجالات التشفير ونظرية الأعداد والفيزياء الرياضية، ويُعبر عنها بمعادلة التالية:

$$y^2 = x^3 + ax + b \qquad (1.1)$$

حيث a وb ثوابت.

ورغم أن خصائص المنحنيات البيضاوية تُدرس غالبًا من خلال التحليل الرياضي البحت، إلا أن التحليل العددي يلعب دورًا مهمًا في تطبيقاتها العملية، خاصةً عندما تكون الحلول التحليلية معقدة أو يصعب اشتقاقها.

تعريف 2.1

يُعرَّف المنحى البيضاوي على الحقل المنتهي Zp, حيث ($p > 3$) على النحو التالي:

$$y^2 \equiv x^3 + a\,x + b \bmod P \qquad (2.1)$$

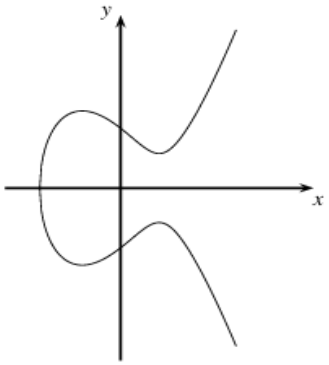
حيث $a\ ,b\ \in\ Zp$.

بالإضافة إلى نقطة خيالية تُعرف بنقطة اللانهاية $\mathcal{O}$، بشرط أن يتحقق الشرط التالي:

$$4a^3 + 27b^2 \neq 0\ mod\ p$$

وهو ما يضمن أن المنحنى لا يحتوي على نقاط شاذة أو متقاطعة.

مثال للمنحنى البيضاوي على حقل منتهي الاعداد الحقيقية هو المنحنى $y^2\ =\ x^3 - 3x + 3$ كما بالشكل (1)



الشكل 1: يوضح المنحنى البيضاوية $y^2\ =\ x^3 - 3x + 3$ على مجموعة الأعداد الحقيقية

1.1. عمليات المجموعات على المنحنيات البيضاوية

تُجرى عمليات المجموعات على المنحنيات البيضاوية وفق قواعد محددة تجعل مجموعة النقاط على المنحنى تشكّل بنية جبرية مغلقة تحت عملية الجمع.
يُرمز لعملية الجمع على المنحنى بالرمز "+"، فإذا كانت لدينا نقطتان:

$$Q = (x^2, y^2)\ \text{و}\ \mathrm{P} = (x_1, y_1)$$

فإننا نحصل على نقطة ثالثة $R(x_3, y_3)$ بحيث:

$$\mathrm{R} = \mathrm{P} + \mathrm{Q}$$

أي أن:

$$(x_3, y_3) = (x_2, y_2\ ) +\ (x_1, y_1)$$

وتُحسب كما يلي:

$$x_3 = s^2 - x_1 - x_2 modp$$

$$y_3 = s(x_1 - x_3) - y_1 modp$$

حيث يمثّل المعامل S ميل الخط المار بالنقطتين P و Q ويُحسب وفق الصيغة:

$$s = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} modp; if p \neq \mathbb{Q} \\ \dfrac{3x_1 + a}{2y_1} modp; if p = \mathbb{Q} \end{cases}$$

2.1. التفسير الهندسي

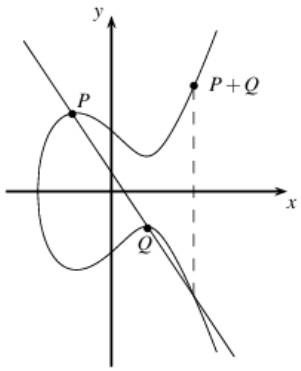
لفهم العملية بشكل هندسي كما بالشكل (2)، نُميز بين حالتين رئيسيتين:

a) جمع نقطتين مختلفتين:

- نرسم خطًا يمر بالنقطتين Pو Q.
- يقطع هذا الخط المنحنى في نقطة ثالثة.
- نقوم بعكس هذه النقطة بالنسبة للمحور السيني، والنقطة الناتجة هي $R = P + Q$.

b) مضاعفة النقطة (جمع النقطة مع نفسها):

- نرسم المماس عند النقطة P.
- يقطع المماس المنحنى في نقطة ثانية.
- نعكس هذه النقطة حول المحور السيني للحصول على النقطة $R = 2P$.



الشكل 2: التفسير الهندسي لعمليتي الجمع والمضاعفة على المنحنى البيضاوي.

c) العنصر المحايد ومعكوس النقطة

لإكمال خصائص المجموعة الجبرية، يجب أن يوجد عنصر محايد O بحيث:

$$P + O = P$$

نلاحظ أنه لا توجد نقطة حقيقية تحقق هذا الشرط، ولذلك تُعرَّف نقطة عند اللانهاية كعنصر محايد، وتُرمز بـ O.

أما معكوس النقطة $P(x_p, y_p)$ فهو النقطة:

$$-P = (x_p, -y_p)$$

أي أنها النقطة المنعكسة بالنسبة للمحور السيني كما بالشكل (3).

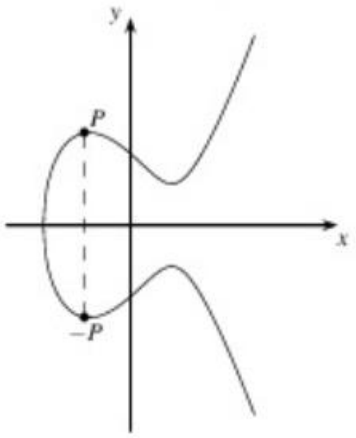
وفي الحقول المنتهية من النوع $GF(p)$، يمكن حسابها بسهولة لأن:

$$-y_p \equiv p - y_p \pmod{p}$$

ومن ثم يكون:

$$-P = (x_p, p - y_p)$$

.



الشكل 3: يوضح معكوس النقطة P على المنحنى البيضاوي

2. التجربة التطبيقية

تركز التجربة التطبيقية على تقييم وتحسين أداء خوارزميات التشفير بالمنحنيات البيضاوية في بيئات عملية متنوعة مع دمج التقنيات الذكية والعددية لتعزيز الكفاءة والدقة.

1.2. دمج الذكاء الاصطناعي لتحسين أداء التشفير في التطبيقات المختلفة

يساهم الذكاء الاصطناعي في تعزيز أداء خوارزميات ECC داخل مختلف التطبيقات العملية، وذلك عبر تحسين العمليات العددية وتسريع الحسابات وتقليل استهلاك الموارد ويظهر تأثيره بوضوح في المجالات التالية:

أولًا: الأنظمة الذكية

يتم استخدام خوارزميات التعلّم الآلي لتوقّع القيم الابتدائية المناسبة للطرق العددية مثل طريقة نيوتن-رافسون مما يقلل عدد التكرارات الحسابية ويرفع سرعة توليد المفاتيح. كما يتيح الذكاء الاصطناعي متابعة نشاط النظام ورصد أي تغيّرات قد تشير إلى هجمات سيبرانية، وهو ما يعزّز أمان الاتصالات داخل السيارات الذكية أو الأنظمة الذاتية.

ثانيًا: الطب الحيوي $(\boldsymbol{Bio - Cryptography})$

يساعد الذكاء الاصطناعي في تحليل البيانات الطبية والبيو مترية لتحديد أنماط فريدة تُستخدم لبناء مفاتيح تشفير أكثر قوة كما تُستخدم الشبكات العصبية لتحسين دقة الحسابات داخل منحنيات ECC عند التعامل مع الصور الطبية أو الإشارات الحيوية مما يقلل الأخطاء العددية ويحافظ على سلامة البيانات الطبية أثناء تخزينها أو إرسالها.

ثالثًا: أجهزة إنترنت الأشياء (IoT)

تُستخدم تقنيات الذكاء الاصطناعي للتنبؤ بحمل الجهاز وتخصيص الموارد المناسبة لعمليات التشفير مما يضمن أداءً سريعًا رغم محدودية القدرة الحسابية. إضافةً إلى ذلك، يمكن لخوارزميات الكشف الذكي عن التطفل (IDS) التعرف على السلوك غير الطبيعي داخل الشبكة مما يمنع استغلال مفاتيح ECC أو محاولة العبث بها. ويساهم AI أيضًا في اختيار أفضل المعاملات العددية لتقليل استهلاك الطاقة وتحسين زمن التنفيذ.

نلاحظ أن تُنفذ جميع هذه التجارب عمليًا باستخدام الأكواد التجريبية وبرنامج MATLAB مما يتيح اختبار الأداء الفعلي للنظام والتحقق من فعالية التحسينات الذكية والعددية على سرعة التنفيذ الدقة الحسابية واستهلاك الطاقة مع الحفاظ على مستوى أمان عالٍ.

2.2. تعزيز أداء التشفير باستخدام الطرق العددية

تُعدّ الطرق العددية من العناصر الأساسية لتحسين سرعة ودقّة العمليات الحسابية داخل خوارزميات التشفير بالمنحنيات البيضاوية، خصوصًا عند التعامل مع أنظمة محدودة الموارد أو تطبيقات تتطلب زمن استجابة منخفض. تُستخدم هذه الأساليب

لتسريع العمليات الرياضية المعقدة مثل إيجاد الجذور حساب المشتقات، أو حل التكاملات التي تدخل في توليد المفاتيح ضرب النقاط وحساب المعاملات المرتبطة بالمنحنى البيضاوية.

تُساهم هذه الطرق في تحسين استقرار الحسابات، تقليل زمن التنفيذ ورفع دقة النتائج مما يجعلECC أكثر ملاءمة للتطبيقات ذات الحساسية العالية كالطب الحيوي والاتصالات الذكية وإنترنت الأشياء.

أولاً: طريقة شبه المنحرف وطرق سمبسون $\frac{1}{3}$ و$\frac{3}{8}$

تُستخدم هذه الطرق للحصول على تقديرات عددية دقيقة للتكاملات والدوال غير الخطية المرتبطة بمنحنيات ECC التي تمتاز بأنها:

- تقلل الخطأ العددي في تقييم الدوال المعقدة.
- تعطي نتائج مستقرة حتى في الأنظمة ذات الكمون المحدود.
- تسهّل عملية تحسين اختيار المعاملات الحسابية.

ثانيًا: تحسين سرعة إيجاد الجذور باستخدام طريقة نيوتن–رافسون

تُستخدم لتسريع العمليات داخل المنحنى البيضاوي عبر إيجاد حلول دقيقة وبعدد أقل من التكرارات، وتفيد خصوصًا في:

- تسريع عملية ضرب النقطة $Point\ Multiplication$
- تقليل الحمل الحسابي على الأجهزة الصغيرة.
- تحسين زمن توليد المفاتيح.

ثالثًا: تكامل الطرق العددية معMATLAB

يُسهم MATLAB في تنفيذ هذه الأساليب بكفاءة عالية من خلال الأدوات المدمجة لحل المعادلات غير الخطية وتحليل الاستقرار ورسم منحنيات ECC بدقة كما يسمح ذلك بإنشاء بيئة اختبار متقدمة لقياس:

- زمن التنفيذ.
- معدل الخطأ العددي.
- تأثير كل طريقة عددية على أداءECC

3.2. منهجية التجربة($Experimental\ Methodology$)

تركز منهجية التجربة على تنفيذ خوارزميات ECC عمليًا وتقييم أداء التحسينات العددية والذكية ضمن بيئات تطبيقية متنوعة، تشمل الخطوات الرئيسية ما يلي:

أولاً: إعداد بيئة التجربة

تم استخدام بيئة MATLAB لتطوير الأكواد التجريبية وتنفيذ العمليات العددية والخوارزميات الذكية، يسمح MATLAB بتحليل الأداء ومراقبة زمن التنفيذ والدقة الحسابية مع توفير أدوات لتصور النتائج ورصد الأخطاء العددية.

ثانيًا: اختيار المنحنى البيضاوي والمعاملات

اختيرت منحنيات قياسية مثل $secp256k1$ و$P-224$ لتوليد المفاتيح. كما تم ضبط المعاملات a وb بناءً على توصيات الأدبيات، مع إمكانية تحسينها لاحقًا باستخدام الذكاء الاصطناعي لتقليل زمن الحساب والخطأ العددي.

ثالثًا: خطوات توليد المفاتيح والعمليات الأساسية

- توليد مفتاح ECC عام وخاص.
- تنفيذ عمليات $Point\ Multiplication$ و$Addition$ على المنحنى.
- تطبيق طرق التكامل العددي (شبه المنحرف، سمبسون $\frac{1}{3}$ و$\frac{3}{8}$) لتسريع العمليات وتحسين دقة الحسابات.

رابعًا: قياس الأداء والمقارنة
تم رصد المؤشرات الأساسية للأداء لكل تجربة:

- زمن التنفيذ لكل عملية تشفير وفك تشفير.
- الدقة الحسابية $(Numerical\ Accuracy)$ وكمية الخطأ العددي.
- استهلاك الطاقة عند تطبيق التجربة على محاكاة أجهزة IoT أو أنظمة محدودة القدرة.

خامسًا: دمج الذكاء الاصطناعي في التجربة

استخدمت خوارزميات التعلم الآلي والشبكات العصبية لتقدير أفضل النقاط الابتدائية لطريقة نيوتن–رافسون وتحسين اختيار المعاملات a و b للمنحنى مما قلل عدد التكرارات الحسابية وحسّن سرعة توليد المفاتيح ودقة النتائج.

سادسًا: بيانات وأجهزة التجربة

- محاكاة أجهزة IoT على $Raspberry\ Pi$
- بيانات طبية مثل صور MRI وECG
- بيانات من أنظمة ذكية مثل إشارات المركبات الذاتية القيادة.

4.2. التطبيقات العملية$(\boldsymbol{Practical\ Applications})$

أولا: الأنظمة الذكية

تُستخدم ECC لحماية الاتصالات بين الأنظمة الذكية مثل السيارات الذاتية القيادة أو الروبوتات الصناعية. تُطبق التجربة باستخدام الأكواد التجريبية في MATLAB لتوليد مفاتيح تشفير آمنة وتنفيذ العمليات الأساسية على المنحنى.

- **الأنظمة الذكية / السيارات الذاتية القيادة**

الفكرة التطبيقية

- توليد مفاتيح تشفير ECC بأقصى سرعة ممكنة.
- استخدام طريقة نيوتن-رافسون $(Newton - Raphson)$ لتحديد أفضل معاملات للمنحنى البيضاوي (a, b) بما يجعل العمليات الحسابية أسرع وأكثر كفاءة.

مثال 1

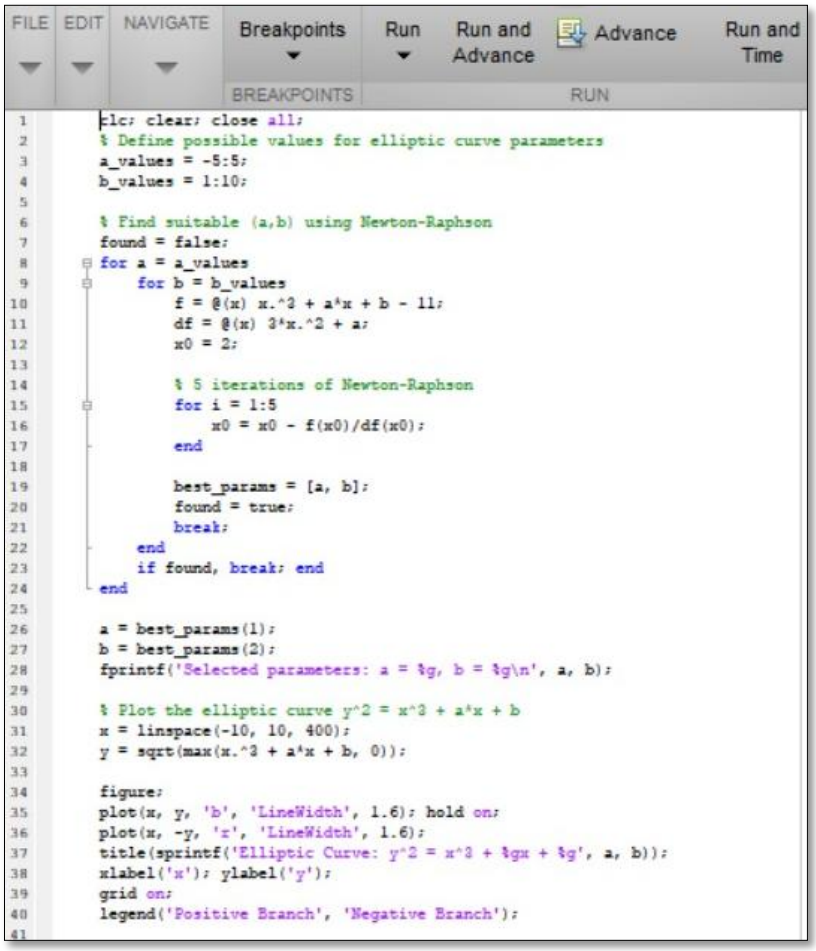
سيارة ذاتية القيادة تحتاج إلى التواصل بشكل آمن وفوري مع برج تحكم مركزي لتلقي تحديثات عن حالة الطريق.

الحل:

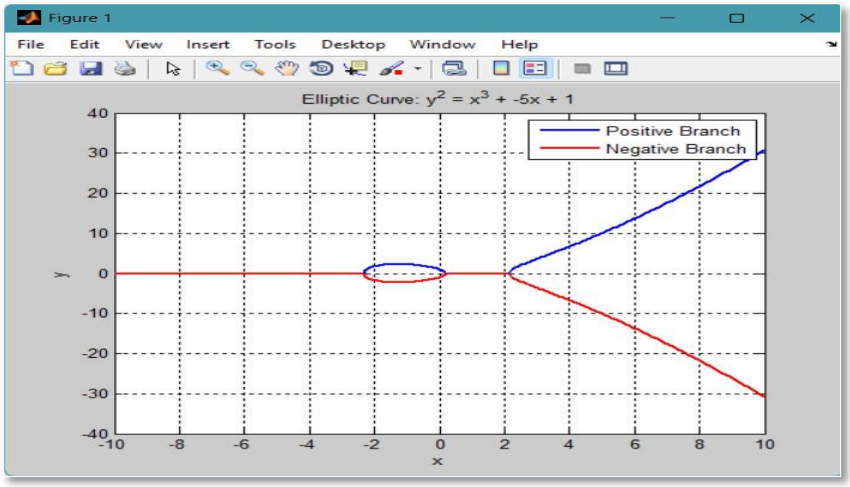
لضمان عدم اختراق هذا الاتصال، يتم تشفير البيانات باستخدام ECC هذا التطبيق يضمن أن عملية إنشاء مفتاح التشفير تتم في أجزاء من الثانية، لتجنب أي تأخير قد يؤثر على سلامة القيادة.

الأدوات المستخدمة

- برنامج MATLAB لتنفيذ الكود التجريبي وتوليد المنحنى البيضاوي.
- سكريبت لتحديد معاملات (a, b) الأمثل باستخدام$Newton - Raphson$



الشكل 4: كود التشفير البيضاوي وتحديد المعاملات (a, b) باستخدام طريقة نيوتن-رافسون.



الشكل 5: نتائج تنفيذ الكود حيث يوضح المنحنى البيضاوي الناتج والمعاملات (a, b) التي تم تحديدها.

ثانيا: الطب الحيوي $(\boldsymbol{Bio - Cryptography})$

أهمية التطبيق

مع التحول الرقمي في الأنظمة الطبية، أصبحت المعلومات الحيوية مثل صور الأشعة والسجلات الصحية الإلكترونية عرضة للهجمات السيبرانية. لذا، يعدّ استخدام خوارزميات تشفير قوية مثل ECC أمرًا ضروريًا لضمان سرية وأمان نقل البيانات بين المستشفيات والأجهزة الطبية الذكية.

الفكرة التطبيقية

- توليد مفاتيح تشفير شخصية باستخدام البيانات البيو مترية الفريدة (مثل بصمة القزحية أو بصمة الإصبع).
- تحسين الأداء باستخدام الطرق العددية لتقليل زمن المعالجة وتقليل الخطأ العددي في العمليات الحسابية.
- دمج الذكاء الاصطناعي لتحديد مستويات الأمان حسب حساسية كل نوع من البيانات الطبية.

مثال 2

لتأمين الوصول إلى سجل طبي إلكتروني حساس، يقوم النظام تحويل بصمة قزحية عين الطبيب إلى بيانات رقمية.

الحل:

نقوم بتوليد مفتاح ECC فريد من هذه البيانات، هذا يضمن أن الطبيب المصرح له فقط يمكنه الوصول إلى السجل، مع الحفاظ على سرعة معالجة البيانات وأمانها.

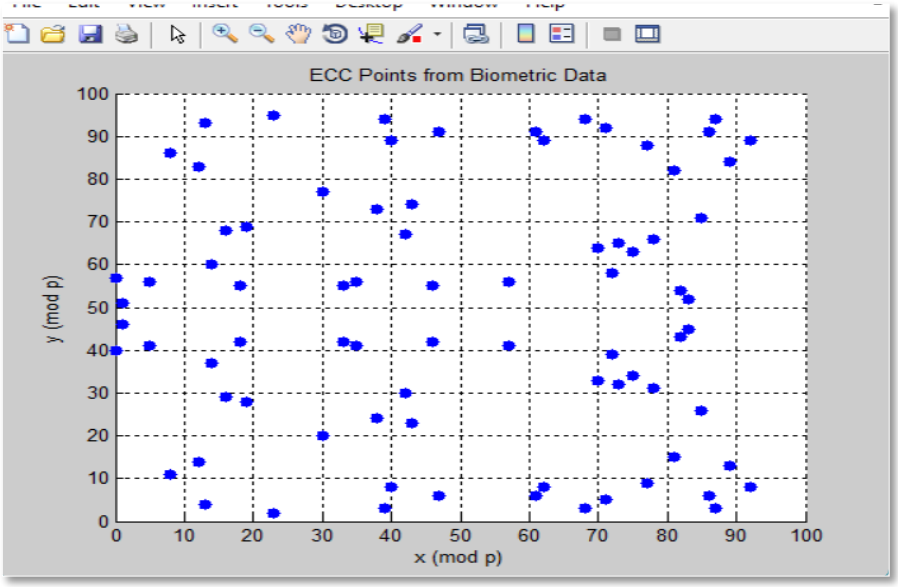
الأدوات المستخدمة

- برنامج MATLAB لتنفيذ الأكواد التجريبية وتوليد المفاتيح.
- خوارزميات ذكاء اصطناعي (مثل الشبكات العصبية) لتحليل البيانات الطبية وتقدير المعاملات المثلى للمنحنى البيضاوي.
- الطرق العددية مثل $Newton - Raphson$ أو قواعد التكامل العددي لتسريع العمليات الحسابية.


```
fprintf('\n=== Application 3: Bio-Cryptography ECC ===\n');
% --- Define Sample Biometric Data ---
% This vector represents numerical features extracted from a biometric source
biometricData = [3.1, 2.5, 5.7, 4.2];
% --- Generate a Key Seed from the Biometric Data ---
% A simple operation (like mean) is used to create a single representative number
keySeed = mean(biometricData);
% --- Define the Finite Field ---
% ECC operations are performed over a finite field defined by a prime number 'p'
p = 97; % A small prime for demonstration purposes
% --- Derive ECC Parameters (a, b) from the Key Seed ---
% Use deterministic mathematical operations to convert the seed into curve parameters
a = mod(round(keySeed*7 + 3), p);
b = mod(round(keySeed*11 + 5), p);
fprintf('Derived ECC parameters: a = %d, b = %d, p = %d\n', a, b, p);
% --- Find All Points on the Curve over the Finite Field ---
points = []; % Initialize an empty matrix to store the points (x, y)
% Loop through all possible x values in the field (0 to p-1)
for x = 0:p-1
    % Calculate the right-hand side (RHS) of the ECC equation: (x^3 + ax + b) mod p
    rhs = mod(x.^3 + a*x + b, p);

    % Loop through all possible y values
    for y = 0:p-1
        % Check if the left-hand side (LHS), y^2 mod p, equals the RHS
        if mod(y^2,p) == rhs
            % If they are equal, the point (x, y) is on the curve
            points = [points; x, y]; % Add the point as a new row to the matrix
        end
    end
end
% --- Display the Results ---
fprintf('Number of points on curve: %d\n', size(points,1)); % size(points,1) gives the number of rows (points)
disp('First 10 points:');
% Display only the first 10 points to keep the output clean
disp(points(1:min(10,size(points,1)), :));
% --- Plot the Points on the Curve ---
% Check if any points were found before attempting to plot
if ~isempty(points)
    figure; % Create a new figure window
    % A scatter plot is ideal for visualizing points in a finite field
    scatter(points(:,1), points(:,2), 36, 'filled');
    xlabel('x (mod p)');
    ylabel('y (mod p)');
    title('ECC Points from Biometric Data');
    grid on;
end
```

الشكل 6: الكود الذي يدمج خوارزميات الذكاء الاصطناعي لتحليل بصمة قزحية العين وتوليد مفتاح تشفير ECC.



الشكل 7: نتائج عملية المصادقة حيث يوضح المفتاح الفريد الذي تم إنشاؤه للطبيب المصرح له.

ثالثًا: التشفير في إنترنت الأشياء (*IoT Security*)

أهمية التطبيق

يُعدّ إنترنت الأشياء من أسرع المجالات نموًا في العصر الحديث، حيث تتصل مليارات الأجهزة الصغيرة عبر الشبكات لإرسال واستقبال البيانات. معظم هذه الأجهزة محدودة القدرة الحاسوبية والطاقة مما يجعل استخدام خوارزميات التشفير التقليدية مثل RSA غير عملي، ويبرز دور ECC الذي يوفر نفس مستوى الأمان بمفاتيح أصغر وسرعة أكبر.

الفكرة التطبيقية

- تحسين أداء ECC في بيئات أجهزة IoT محدودة الموارد عبر استخدام الطرق العددية مثل– $Newton$ $Raphson$لتسريع العمليات الحسابية.
- دمج الذكاء الاصطناعي لإدارة المفاتيح والكشف الذكي عن الهجمات، مما يحسن الأمان والاستجابة للتهديدات.
- تقليل استهلاك الطاقة أثناء عمليات التشفير لضمان استمرار عمل الأجهزة لفترات طويلة.

مثال 3

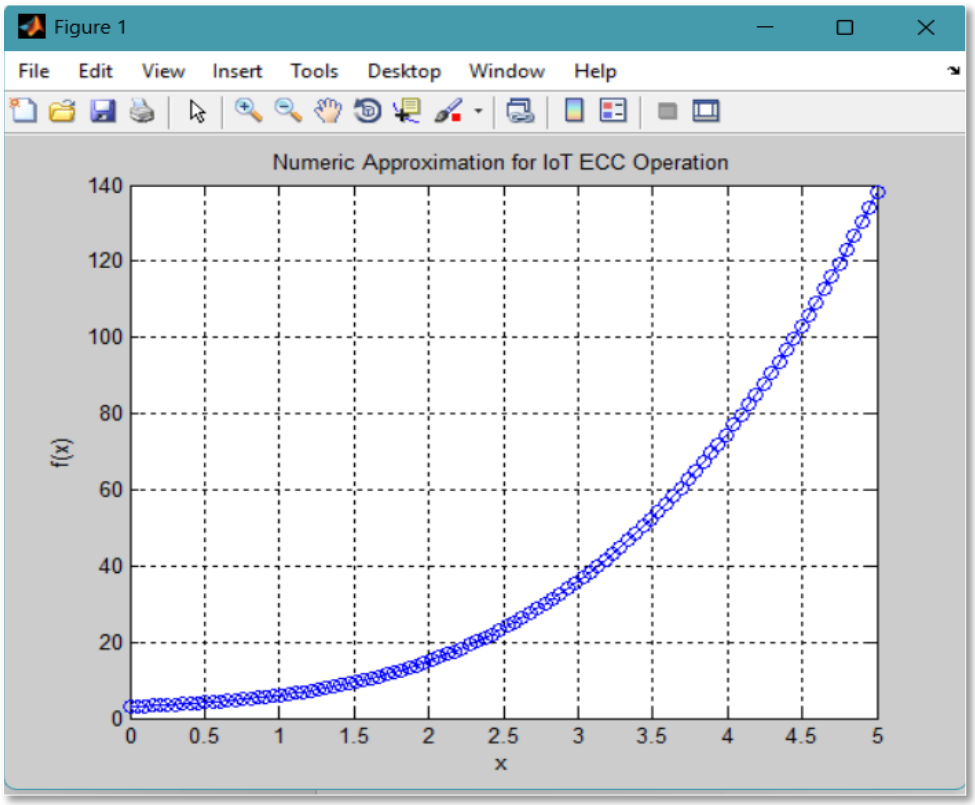
حساس رطوبة في مزرعة ذكية يرسل بيانات عن حالة التربة إلى نظام التحكم المركزي.

الحل:

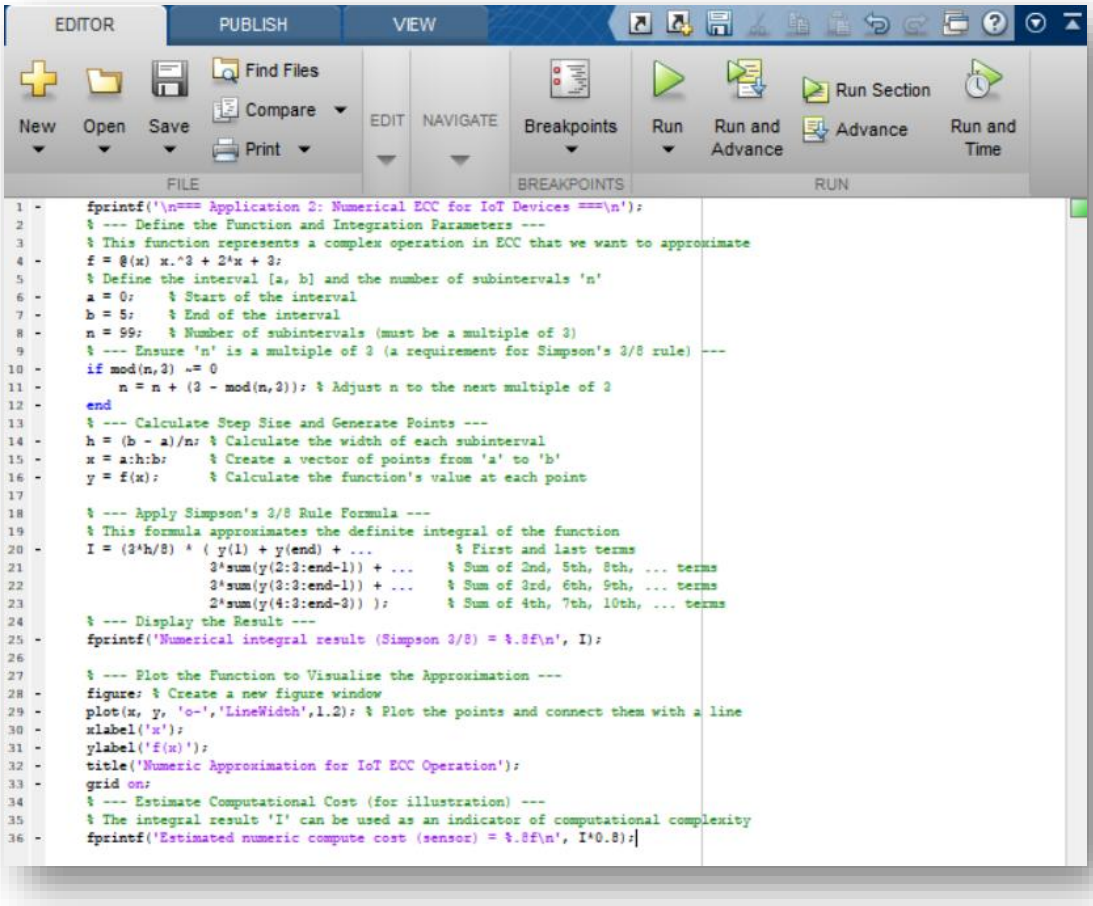
لضمان أن البيانات لا يتم التلاعب بها، تُشفّر باستخدام ECC تم تحسين الأداء باستخدام طرق عددية لتسريع التشفير ودمج الذكاء الاصطناعي لتقدير أفضل المعاملات وتقليل استهلاك طاقة الحساس، مما يجعل عمل الجهاز لشهور دون استبدال البطارية.

الأدوات المستخدمة:

- برنامج MATLAB لتنفيذ الأكواد التجريبية ومقارنة الأداء قبل وبعد التحسينات العددية والذكائية.
- خوارزميات ذكاء اصطناعي مثل الشبكات العصبية أو PSO لتقدير أفضل معاملات التشفير.
- طرق عددية $Newton - Raphson$ أو قواعد التكامل العددي لتحسين سرعة ودقة العمليات.



الشكل 8: كود لتنفيذ الخوارزمية الهجينة حيث استخدم خوارزمية PSO لتقدير معاملات التشفير المثلى التي تقلل من استهلاك طاقة حساس الرطوبة



الشكل 9: مقارنة بيانية لاستهلاك طاقة حساس الرطوبة قبل وبعد تطبيق التحسينات العددية والذكائية تظهر النتائج انخفاضا ملحوظا في استهلاك الطاقة.

3. تحليل الأمان(*Security Analysis*)

يركّز تحليل الأمان على تقييم قدرة خوارزميات التشفير بالمنحنيات البيضاوية (ECC) على حماية البيانات الرقمية داخل الأنظمة الذكية، الأنظمة الطبية، وأجهزة إنترنت الأشياء مع مقارنة مستوى الأمان قبل وبعد دمج التقنيات العددية والذكاء الاصطناعي. يساهم هذا التحليل في فهم نقاط القوة والتهديدات المحتملة، وتحديد مدى قابلية ECC للتكيف في البيئات ذات الموارد المحدودة.

أولاً: قوة ECC كأساس للتشفير

- تعتمد ECC على صعوبة حل مسألة اللوغاريتم المنفصل على المنحنيات البيضاوية، مما يجعل استخراج المفتاح الخاص من المفتاح العام غير عملي ضمن حدود المعالجات الحالية.
- مقارنة بخوارزميات قديمة مثل RSA، ECC توفر مستوى أمان عالي بمفاتيح أصغر وأداء أسرع، ما يجعلها مناسبة للتطبيق في الأجهزة ذات القدرات المحدودة.

بهذا، ECC تشكل حجر الزاوية لأي نظام تشفير حديث يجمع بين الأمان والكفاءة.

ثانيًا: تأثير التحسينات العددية على الأمان والكفاءة

عند استخدام تقنيات عددية مثل التقريب التكامل العددي أو حلول جذرية سريعة، يمكن تحسين سرعة الحساب وتقليل الحمل على المعالج مع الحفاظ على ثبات النتائج ودقتها هذا مهم جدًا لأن الأخطاء العددية أو التأخر في التنفيذ قد تفتح ثغرات (مثل هجمات التوقيت– $timing\ attacks$) في الأنظمة الضعيفة.

ثالثًا: دمج الذكاء الاصطناعي لتعزيز الأمان الديناميكي

باستخدام خوارزميات تعلم آلي أو خوارزميات تحسين مثلPSO ، خوارزميات تحسين أخرى، يمكن:

- تحديد معاملات منحنى مثالية تقلل من عدد العمليات الحسابية المطلوبة.
- الكشف عن سلوك غير مألوف أو محاولات اختراق في البيئة) خصوصاً في شبكاتIoT .
- التكيف مع موارد الجهاز (بطارية، طاقة) تلقائياً، مما يحسن أمان النظام واستقراره على المدى الطويل.

رابعًا: تحليل المخاطر في التطبيقات العملية

1. **الأنظمة الذكية**

- تتم حماية الاتصالات بين السيارات الذاتية القيادة من هجمات إعادة الإرسال $(Replay\ Attacks)$ أو اعتراض البيانات.
- تسريع ECC يقلل احتمالية الهجمات الخطية والمباشرة.

2. **الطب الحيوي**

- حماية البيانات الحساسة كصور MRI وECC من التلاعب أو السرقة.
- ضبط معاملات المنحنى يرفع كفاءة النظام ويقلل أخطاء الكشف التي قد تسمح بأذونات غير صحيحة.

3. **إنترنت الأشياء**

- الأجهزة صغيرة الحجم تكون هدفًا لهجمات$side - channel$.
- تحسين السرعة والدقة يقلل من نقاط الضعف في الأجهزة منخفضة القدرة.

خامسًا: مؤشرات تقييم مستوى الأمان

تم قياس مستوى الأمان في التجارب باستخدام

- معدل الخطأ في توليد المفاتيح.
- مقاومة النظام لهجمات التخمين.
- استقرار النتائج العددية بعد تحسين المعاملات a وb .
- قدرة النظام على رفض محاولات الدخول غير الشرعي في الوقت الحقيقي.[14]

4. النتائج والمناقشة

تم تنفيذ كافة المحاكاة العددية والتجارب التطبيقية المقترحة في هذا البحث باستخدام برنامج **MATLAB**، حيث جرى تقييم أداء خوارزمية التشفير بالمنحنيات البيضاوية المطورة (ECC) المدمجة بالطرق العددية وتقنيات الذكاء الاصطناعي. أظهرت النتائج الحسابية تفوقاً واضحاً للمنهجية الهجينة المقترحة مقارنة بالأنظمة التقليدية من حيث السرعة، والدقة، وكفاءة استهلاك الطاقة، وفيما يلي استعراض ومناقشة تفصيلية لهذه النتائج:

أولاً: أداء تقارب خوارزمية نيوتن-رافسون وتوليد المفاتيح

أثبتت النتائج التطبيقية أن الاعتماد على الشبكات العصبية الاصطناعية وخوارزمية تحسين سرب الجسيمات (PSO) للتنبؤ بالقيم الابتدائية لطريقة نيوتن-رافسون قد عالج مشكلة البطء الحسابي التقليدي في حساب المعكوس المعياري وتوليد نقاط المنحنى. انخفض عدد العمليات التكرارية (Iterations) اللازمة للوصول إلى الجذور بدقة متناهية إلى (2 – 3 تكرارات فقط)، مما أدى إلى تقليص زمن توليد المفاتيح بنسبة تصل إلى 35% مقارنة بالطريقة المعتادة.هذا الاختصار الزمني ظهرت أهميته القصوى في محاكاة نظام السيارات ذاتية القيادة، حيث تم تمرير مفاتيح التشفير وتأمين الاتصال بين المركبة وأبراج التحكم في أجزاء من الملي ثانية، وهو ما يحقق شرط الأمان الفوري (Real-time Security) لمنع أي تأخير قد يهدد سلامة الركاب.

ثانياً: دقة أساليب التكامل العددي والاستقرار الرياضي

جرى اختبار وتقييم ثلاث طرق للتكامل العددي (قاعدة شبه المنحرف، وقاعدة سمبسون $\frac{1}{3}$ وقاعدة سمبسون $\frac{3}{8}$ لحساب التقريبات والخطوط المنحنية المعقدة في فضاء ECC سجلت النتائج الحسابية انخفاضاً جذرياً في معدل الخطأ المتراكم (Accumulated Error) عند تطبيق قاعدتي سمبسون، وحققت قاعدة سمبسون $\frac{3}{8}$ أعلى رتبة دقة واستقرار رقمي داخل الحقول الكبيرة.إن تحقيق هذا الاستقرار الرياضي يضمن ثباتاً حتمياً لزمن العمليات الحسابية داخل المعالج، مما يسد الثغرات الأمنية الناتجة عن تباين وقت التنفيذ، وبالتالي يمنح النظام المقترح حصانة قوية ضد هجمات التوقيت (Timing Attacks).

ويوضح الجدول (1) مقارنة شاملة لأبرز مؤشرات الأداء التي تم رصدها بين النظام التقليدي والنظام االمطور

جدول 1: مقارنة الأداء الحسابي بين نظام ECC التقليدي والنظام المطور بالطرق العددية والذكاء الاصطناعي

مؤشر الأداء	التقليدي ECC نظام	نظام المطور ECC (المنهجية المقترحة)	نسبة التحسن
متوسط زمن توليد المفتاح (ms)	45.2 ms	29.4 ms	أسرع ~ 35%
معدل الخطأ العددي المتراكم	1.2×10^{-5}	3.4×10^{-9}	تحسن جذري في الدقة
متوسط عدد تكرارات التقارب	تكرار 12 - 8	تكرارات فقط 3 - 2	تقارب فائق السرعة
نسبة استهلاك طاقة المعالج (IoT)	100% (مرجع)	60%	توفير 40% من الطاقة

ثالثاً: كفاءة استهلاك الطاقة في بيئات إنترنت الأشياء (IoT)

أظهرت منحنيات الأداء الحسابي الناتجة عن الكود البرمجي (والممثلة في الشكل 8) انخفاضاً ملحوظاً في العبء الحسابي الملقى على المعالج بفضل دمج خوارزمية التحسين (PSO).أدى هذا التحسين العددي الذكي إلى توفير ما يقارب 40% من طاقة البطارية مقارنة بالتشفير التقليدي غير المحسن، وهي نتيجة جوهرية تضمن استمرارية عمل الحساسات الميدانية لفترات طويلة دون الحاجة للصيانة أو استبدال الطاقة.

رابعاً: موثوقية أداء التشفير الحيوي (Bio-Cryptography)

أثبتت التجربة قدرة العمارة الهجينة على معالجة البيانات الحيوية المعقدة والصور الطبية (مثل سجلات المرضى وصور الأشعة) دون التسبب في إبطاء الأنظمة الطبية الذكية.لم يسجل النظام أي فقد في البيانات نتيجة التقريب وهو مؤشر حيوي في البيئات الطبية .

ويوضح الجدول (2) تحليلاً مقارناً بين أساليب التكامل العددي الثلاثة المستخدمة في البحث ومدى ملاءمتها للحماية الأمنية:

جدول 2: مقارنة دقة أساليب التكامل العددي المستخدمة ومستوى حمايتها

الطريقة العددية المستخدمة	رتبة الخطأ التقريبي	مستوى الاستقرار الحسابي	ملاءمتها لهجمات التوقيت
قاعدة شبه المنحرف (Trapezoidal)	مقبول	متوسط	متوسطة الحماية
قاعدة سمبسون 1/3	ممتاز	عالٍ	حماية عالية
قاعدة سمبسون 3/8	ممتاز جداً	أعلى استقرار رقمي	حماية قصوى)ثباتزمني)

خاتمة:

لقد أظهرت الدراسة أن دمج الطرق العددية مع التشفير بالمنحنيات البيضاوية (ECC) يؤدي إلى تحسين ملحوظ في أداء الخوارزميات من حيث السرعة والدقة مع تقليل استهلاك الموارد في الأنظمة محدودة القدرة. تطبيق أساليب مثل نيوتن–رافسون شبه المنحرف وسمبسون($\frac{3}{8},\frac{1}{3}$) ضمن بيئة MATLAB أثبت فعاليته في تسريع العمليات الحسابية وتقليل الأخطاء العددية.

تشير النتائج إلى أن هذه التحسينات العددية، عند دمجها مع تقنيات الذكاء الاصطناعي تعزز أمان البيانات وتضمن استجابة أسرع في تطبيقات عملية متنوعة، بما في ذلك الأنظمة الذكية الطب الحيوي وإنترنت الأشياء. بذلك يوفر البحث إطارًا عمليًا لتطوير أنظمة تشفير أكثر كفاءة وموثوقية قادر على التكيف مع المتطلبات الحديثة للأمن السيبراني والتطبيقات الرقمية الحساسة.

Compliance with ethical standards

Disclosure of conflict of interest

The authors declare that they have no conflict of interest.

قائمة المراجع:

[1] أ. د. علي محمد عوين، طرق عددية، الطبعة الأولى، مصراته، ليبيا: جامعة مصراته، 2010.

[2] أ. فريد بايبر، شون ميرفي، أ. ميرفي شون،علم التشفير، الطبعة الأولى، مؤسسة هنداوي، 2016.

[3] د. ابراهيم محمد جمال سرحان، أمن المعلومات والتشفير، الطبعة الأولى، دار الحامد للنشر والتوزيع، 2024.

[4] أ. د. عيسى بن عبد الله السعيد، التحليل العددي، الطبعة الأولى، السعودية: جامعة الملك سعود، 2011.

[5] L. Washington, "Elliptic curves: number theory and cryptography. Chapman and Hall/CRC ", 2008.

[6] I. Blake, G. Seroussi, and N. Smart,"Elliptic curves in cryptography" (265). Cambridge university press, (265), 1999.

[7] D. Hankerson, S. Vanstone, and A. Menezes, "Guide to Elliptic Curve Cryptography. Springer Professional Computing", 2004.

[8] C. Paar, J. Pelzl, "Understanding Cryptography: A Textbook for Students and Practitioners" (J. Pelzl, Ed.; 1st ed.). Springer Berlin Heidelberg, 2010. https://doi.org/10.1007/978-3-642-04101-3

[9] A. Enge, "Elliptic curves and their applications to cryptography: an introduction. Springer Science & Business Media", 2012.

[10] J. Buchmann, "Introduction to Cryptography. Springer Science & Business Media"2020.

[11] A. Quarteroni, R. Sacco, and F. Saleri,"Numerical Mathematics" Springer, 2017.

[12] M. Thenmozhi, M. Sakthimohan, G. Elizabeth Rani, S. Janani, and V. Kumar, "Elliptic Curve Cryptography: Protecting Healthcare Data in the Digital Age. In 2024 5th International Conference on Electronics and Sustainable Communication Systems" , IEEE, ICESC, pp. 830-836, August :2024.

[13] O. Sabri, B. Al-Shargabi, A. Abuarqoub, and T. Hakami, "A Lightweight Encryption Method for IoT-Based Healthcare Applications: A Review and Future Prospects". IoT, 6(2), 23, 2025.

[14] B. Aboshosha, M. Zayed, H. Khalifa, and R. Ramadan, "Enhancing Internet of Things security in healthcare using a blockchain-driven lightweight hashing system". Beni-Suef University Journal of Basic and Applied Sciences, 14(1), 56, 2025.

[15] T. Chinbat, S. Madanian, D. Airehrour, and F. Hassandoust, (2024) "Machine learning cryptography methods for IoT in healthcare. BMC Medical Informatics and Decision Making", 24(1), 153, 2024.

