مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (٩) العدد (١٢) ٢٠٢٥
Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (9) No. (12) 2025

نظام توقيع هجين مبني على تحليل مقارن للتواقيع الكمومية والمنحنيات الاهليليجية

د. بســـيم صالح برهوم*

(تاريخ الإيداع ٢٠٢٥/٧/١٥ . قُبِل للنشر في ٢٠٢٥/١٠/٧)

□ ملخّص □

مع عولمة التحول الرقمي الذي بدأ يفرض نفسه في كافة مجالات الحياة وعلى مختلف المستويات وفي كافة بلدان العالم، أصبحنا ملزمين على استخدام العمليات الرقمية على مدار الساعة وهذا يحتم علينا العمل على ضمان سلامة البيانات والمعلومات التي نقوم بتبادلها مع جهات عدة، وأصبحنا ملزمين أيضاً بالتحقق من مصادر هذه البيانات، ومن جهة ثانية فإننا ملزمين بإثبات الهوية الرقمية للأخرين وذلك من أجل كل عملية استقبال للبيانات أو عملية إرسال، وذلك بهدف ضمان حسن سير هذه العمليات بعيداً عن حالات الاختراق والاستغلال، وهذا يتطلب دراسة وافية لخوارزميات التوقيع الرقمي Digital Signature Algorithms واعتماد أفضلها وأنسبها لبيئات العمل، مع الاخذ بعين الاعتبار التكاليف المرافقة ولاسيما مع دخول عصر الحوسبة الكمومية كبيئة عمل جديدة بما تفرضه من تحديات جديدة وكبيرة على كافة مستويات ومتطلبات عصر العولمة الرقمية .

قمنا في هذا البحث بتقييم أداء أهم خوارزميات التوقيع الرقمي المعتمدة على المنحنيات الاهليليجية (خوارزمية **ECDSA**) ومدى قابليتها لتحسين المستوى الأمني الذي يمكن أن تؤمنه في عصر الحوسبة الكمومية، وخوارزميات إنتاج التواقيع الكمومية المعتمدة على شبكات لاتس Lattice Networks (خوارزمية Falcon)، ومن ثم إجراء مقارنة عملية بين الأسلوبين في التوقيع الرقمي تشمل توليد المفاتيح وإنتاج التواقيع والتحقق من صحتها، إضافة إلى مقارنة حاجة كل منهما للموارد في بيئات مختلفة وصولاً الى اقتراح نظام توقيع هجين يستفيد من إيجابيات كلا الأسلوبين ويغطي فترة انتظار ظهور وتوفر الحواسيب الكمومية بشكلها التجاري .

الكلمات المفتاحية : FALCON algorithm ، ECDSA algorithm ، التشفير الكمومي ، التوقيع الرقمي ، خوارزميات المنحنيات الاهليليجية ، التشفير مابعد الكمومي ، تشفيرشبكات Lattice .

* عضو هيئة تدريسية – أستاذ مساعد في قسم البرمجيات ونظم المعلومات – كلية الهندسة المعلوماتية – جامعة اللاذقية – سوريا.

مجلة جامعة طرطوس للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (٩) العدد (١٢) ٢٠٢٥
Tartous University Journal for Research and Scientific Studies - engineering Sciences Series Vol. (9) No. (12) 2025

A hybrid signature system based on a comparative analysis of quantum signatures and elliptic curves

Dr: Baseem Saleh Barhoum*

(Received 15/7/2025 . Accepted 7/10/2025)

□ ABSTRACT □

With the globalization of digital transformation that has begun to impose itself across all areas of life, at various levels, and in all countries around the world, we have become obligated to use digital processes around the clock. This necessitates working to ensure the safety of the data and information we exchange with multiple parties. We are also required to verify the sources of this data. On the other hand, we are obligated to prove our digital identity to others for every data reception or transmission operation, with the aim of ensuring the smooth functioning of these processes away from hacking and exploitation incidents. This demands a thorough study of digital signature algorithms and adopting the best ones from a security and performance standpoint, while considering the associated costs—especially with the advent of the quantum computing era as a new working environment, which imposes significant new challenges on all levels and requirements of the digital globalization era.

In this research, we will evaluate the performance of the most important encryption algorithms based on lattice networks, particularly the current digital signature algorithms that rely on elliptic curves through the ECDSA algorithm, and assess their capability to enhance the security level they provide in the quantum computing era. We will also compare this with the performance of the most important quantum-resistant encryption algorithms used in digital signatures, specifically the Falcon algorithm.

Keywords: FALCON algorithm, ECDSA algorithm, Quantum cryptography, Digital signature, Elliptic-curve cryptography, Post-quantum cryptography, Lattice-based cryptography.

* Lecturer – Department of Software and Information Systems – Faculty of Informatics engineering – Tishreen University – Syria.
Email : bbarhoum2@gmail.com

مقدمة

من أهم الاعتبارات الأمنية عند الحديث عن الوثائق بشكلها القديم الورقي أو بشكلها الرقمي سلامة هذه الوثائق (Integrity)، والوثوق بهوية مصدرها (Authentication)، حيث يتم استخدام أنظمة التشفير Encryption من أجل تحقيق هذه الاعتبارات، وتعتبر خوارزميات التوقيع الرقمي القائمة على الرياضيات المتعلقة بالمنحنيات البيانية الاهليليجية هي الأفضل في توليد التواقيع الرقمية والتواقيع الرقمية المختومة زمنياً (Time-stamped signature) في العصر الحالي ومن أهم الخوارزميات التي تبرز في هذه المجال خوارزمية ECDSA (Elliptic Curve Digital Signature Algorithm) ، حيث تضمن سلامة البيانات من التعديل أو التغيير إضافة إلى إثباتها لهوية المرسل او المُوقّع على الرسالة، إضافة إلى امكانياتها العالية في تبادل المفاتيح، ولكن مع التطورات المتسارعة في مجال الحوسبة الكمومية والحواسيب ذات السرعات العالية مقارنة مع الحواسيب المستخدمة حالياً، بدأ الشك بقدرات هذه الخوارزميات على الصمود والعمل بالمستوى الأمني المتناسب مع هذه التقنيات الحديثة، وبدأت تظهر خوارزميات جديدة يطلق عليها خوارزميات ما بعد الكم Post-quantum algorithms ، والتي تعمل وفق المبادئ الكمومية الحديثة ، ومن أهم هذه الخوارزميات تلمع خوارزمية FALCON ، والتي تعتمد في عملها على Lattice Networks وعلى كثيرات الحدود من أجل إنتاج تواقيع رقمية مقبولة الطول ولكنها تحتاج مفتاح طويل نسبياً [1] . سنقدم في هذا البحث مقاربة عملية لتقيم أداء عمل خوارزمية ECDSA في البيئات الحالية ومدى قدرتها على الصمود والمنافسة في البيئات الكمومية ولاسيما في مجال الحفاظ على مستوى أمني مقبول من خلال مجال المفاتيح الذي يسمح لها بزيادة أطوال المفاتيح المستخدمة بشكل ملحوظ وأثر ذلك على الأداء العام للخوارزمية، ومن ثم مقارنة جوانب الأمان والأداء مع مثيلاتها في الخوارزمية الكمومية المقترحة حديثاً FALCON والتي تستخدم سيناريوهات عملية متعددة متعلقة بمفاهيم شبكات لاتس ومفاهيم كثيرات الحدود، وسنقدم أيضاً نظرة مستقبلية عن تطوير أنظمة الحماية من خلال اقترح التواقيع الهجينة hybrid Signatures.

مشكلة البحث

ان مسألة ضمان سلامة المعلومات من التعديل والتزوير أثناء نقلها عبر الوسائط المختلفة، أو أثناء تخزينها، إضافة إلى مسألة التحقق من مصدرها والوثوق بالهوية الرقمية لمرسلها وذلك ضمن شروط الأداء العالي ومتطلبات الموارد البسيطة، ولاسيما في البيئات محدودة الموارد من أعقد المسائل الأمنية التي تفرض تحديات تقنية تتطور باستمرار وقدد ازدادت هذه التحديات في العصر الحالي مع التطور التقني الواسع ولاسيما مع دخول عصر الحوسبة الكمومية الذي أحدث ثورة في سرعة أداء العمليات الحسابية والذي ينبئ بانهيار غالبية أنظمة الحماية التقليدية المتبعة حالياً [2] ، وبالتالي لابد من البحث عن تقنيات وأساليب جديدة يمكنها الوقوف في وجه التحديات المستجدة والصمود في وجه الهجمات الكمومية الجديدة.

هدف البحث

يهدف هذا البحث بشكل أساسي إلى تقييم أداء الخوارزميات الأمنية القائمة على المنحنيات الاهليليجية **(Elliptic Curve)** ، ومقارنة أدائها والمستوى الأمني الذي توفره مع المستوى الأمني وأداء الخوارزميات الأمنية الكمومية في مجال التوقيع الرقمي Digital Signature، ومن ثم اقتراح نظام توقيع هجين مناسب لبيئات العمل الحالية والمستقبلية، وذلك من خلال اتباع الخطوات الآتية:

١- تقييم أداء الخوارزمية ECC التي تعمل على المنحنيات الاهليليجة في مجال التوقيع الرقمي .

٢- تقييم أداء خوارزمية Falcon الكمومية في التوقيع الرقمي .

٣- إجراء تحليل مقارن لأداء الخوارزميتين في بيئات مختلفة .

٤- اقتراح نظام توقيع هجين مكون من الخوارزميتين وخوارزمية إنتاج البصمة الرقمية SHA-512 .

خوارزمية ECC (Elliptic Curve Cryptography)

قدمت الخوارزميات القائمة على فكرة استخدام المنحنيات الاهليليجية مستوى أمني عالي، وأداء متميز مع التمتع بفضاء مفاتيح يسمح بزيادات إضافية في مستويات الأمان من خلال زيادة بسيطة على أطوال المفاتيح المستخدمة، وتعتمد هذه الخوارزميات على تحويل النص إلى نقاط على المنحني، ومن ثم جمع النقاط وفق قوانين خاصة بالمنحنيات.

١- **توليد المفاتيح Key generation:**

-نختار d كمفتاح خاص private key بحيث يكون $1 \leq d \leq n-1$، حيث n عدد أولي يمثل ترتيب نقطة التوليد

-نحسب المفتاح العام public key Q من العلاقة Q = d x G ، حيث G نقطة أساس (نقطة توليد) و هي نقطة محددة على المنحنى الإهليلجي تُستخدم كبداية لعمليات الضرب النقطي (multiplication)، وبحيث تتم عملية الجداء X وفقا لقواعد العمليات على المنحنيات الاهليليجية (جمع متكرر)، و يتم اختيار G بحيث يكون ترتيبها n عدد أولي كبير، مما يجعل عمليات كسر المفتاح شبه مستحيلة من الناحية الحسابية [4] [3] .

٢- **التوقيع Signature:**

-لتوقيع الرسالة m لابد من التوافق على معادلة المنحني من الشكل $y^2 = x^3 + ax + b$ ، وعلى حقل مناسب F_P وعلى نقطة الاساس G، و n عدد صحيح موجب يمثل ترتيب نقطة التوليد G (عدد مرات الجمع المطلوب القيام بها على G من أجل الوصول إلى النقطة الحيادية او ما يسمى نقطة اللانهاية) ، حيث يتم ضرب نقطة الأساس G فيه أي (n . G) ،أي يتم اختيار n بحيث يحقق n.G = O ، ومن ثم نطبق الاجرائية الآتية:

-نوجد بصمة الرسالة بتطبيق خوارزمية الهاش SHA ، أي e= H (m)

-نأخذ من يسار البصمة السابقة n bits ، أي $z=L_n(e)$، بحيث تكون z بطول n .

-نختار عدد سري صحيح عشوائي k من المجال [1 , n-1] ، ويجب اختيار k جديدة من أجل كل توقيع.

-نحسب النقطة $(x_1 , y_1) = k . G$.

-نحسب $r = x_1 \bmod n$ ، واذا كانت r = 0 فإننا نعيد اختيار k .

-نحسب $s = k^{-1} (z + r\, d) \bmod n$ ، وإذا كانت s = 0 فإننا نعيد اختيار k من جديد.

-يكون التوقيع الرقمي هو الثنائية (r , s) [6] [5].

٣- التحقق من التوقيع Verification Signature:

للتحقق من صحة التوقيع (r , s) على بصمة الرسالة m يلزمنا وجود المفتاح العام Q والذي يمثل نقطة على المنحني وخوارزمية إنتاج البصمة المستخدمة عند إجراء عملية التوقيع، ومن ثم نتبع الاجرائية الآتية:

-نتأكد من أن Q يقع على منحني التشفير.

-نتأكد من أن $n \times G = O$ ، حيث n هو عدد صحيح أولي يمثل ترتيب النقطة G.

-نتحقق من أن r و s أعداد صحيحة في المجال [1 , n-1] .

-تحسب هاش الرسالة e' = H(m) .

-تأخذ n bits من يسار e' ، أي $z' = L_n(e')$ ، وذلك عندما يكون طول الهاش أكبر من n

-نحسب $u_1 = z'.s^{-1} mod\ n$ و $u_2 = r.s^{-1} mod\ n$.

-نحسب النقطة $(x_1, y_1) = u_1 \times G + u_2 \times Q$ ، وإذا كانت $(x_1, y_1) = 0$ فإن التوقيع غير صحيح.

-إذا كان $r \equiv x_1 mod\ n$ ، فإن التوقيع صحيح وخلاف ذلك يكون التوقيع غير صحيح [7] [5] [3].

نقدم تلخيص للمفاتيح، وصفة أزمنة توليدها، وإنتاج التوقيع وحجمه والتحقق في خوارزمية ECC في الجدول رقم (١) الآتي:

جدول رقم (١) المواصفات العامة لـ ECDSA

المفتاح الخاص	256 – 528 bits
المفتاح العام	512 – 1056 bits
أكبر طول مفتاح مستخدم	528 bits
أصغر طول مفتاح مقبول	256 bits
توليد المفاتيح	سريع جداً
توقيت التوقيع	سريع جداً
توقيت التحقق	سريع جداً
حجم التوقيع	٥١٢bits – ١٠٥٦

خوارزمية FALCON :

تمثل الحوسبة الكمومية تقنية ناشئة يمكن استغلالها لتنفيذ آليات تشفير وفك تشفير قوية مطلوبة للاتصالات المستقبلية الآمنة، ومع ذلك، فإن قيود الطاقة والموارد تشير إلى أنه يجب تنفيذ خوارزميات محددة موفرة للطاقة وخفيفة.

في رد على التهديد الذي تشكله الحواسيب الكمومية على تشفير المفتاح العام التقليدي أطلق المعهد الوطني للمعايير والتكنولوجيا

National Institute of Standards and Technology (NIST) عملية لتوحيد معايير تشفير المفتاح العام المقاوم للكم، وخوارزميات التوقيع الرقمي. من هنا كان اختيارنا خوارزمية Falcon التي دخلت الجولة

الثالثة في منافسات (NIST) [8]، وتعتمد هذه الخوارزمية على الشبكات الرياضية (lattice-based cryptography) وتحتاج عمليات حسابية مكثفة (ضرب مصفوفات، تحويلات فوريه السريع FFT) ، عمليات توليد المفتاح، التوقيع، والتحقق كلها معقدة نسبياً، و تعتبر من أهم خوارزميات التشفير الكمومي وهي مقاومة جداً للهجمات الأمنية، لذلك فهي مفضلة في تطبيقات التي تتطلب أمان عالٍ [9]

و تعد **FALCON** خوارزمية حديثة مرشحة من قبل المعهد الوطني للمعايير والتكنولوجيا (NIST) لتكون الخوارزمية المعيارية للتوقيع الرقمي [25]، وتعتمد كثيرات الحدود f(x) , g(x) في عملية توليد المفتاح الخاص، ومن ثم الحصول على المفتاح العام h(x)، وهي جزء من مجموعة الخوارزميات المقاومة للهجمات الكمومية، وتتميز FALCON بأداء أمني عالي، مما يجعلها مثالية للتطبيقات الحديثة [10] .

١- **توليد المفاتيح Key Generation :** تتكون عملية توليد المفاتيح في خوارزمية Falcon من :

اختيار المفتاح الخاص Private key

-نختار كثير حدود $f(x)$ قابل للعكس بالقياس q (عدد أولي)، ويجب أن تكون معاملات $f(x)$ صغيرة قياساً مع q

-نختار كثير حدود $g(x)$ ، أيضا ذات معاملات صغيرة قياساً مع q ، و $f, g \in Z[x] / (\phi)$ ، حيث $\phi = x^n + 1$

-يتم ايجاد كثيري حدود F , G بحيث $F, G \in Z[x] / (\phi)$ ويحققان المعادلة $f * G - g * F = q \mod \phi$

حساب المفتاح العام public key

تتم عملية حساب المفتاح العام h(x) بحيث ($\mathbf{h} \in Z_q [x] / (\phi)$) و حيث

$\phi = x^n + 1$ بواسطة العلاقة : $h(x) = g(x) * f^{-1}(x) \mod q$

يتم إيجاد المعكوس $f^{-1}(x) \mod q$ باستخدام خوارزمية إقليدس بما يحقق العلاقة : $f^{-1} = f * 1 \mod q$

٢- **التوقيع Signature:**

تعتمد عملية التوقيع من خلال خوارزمية Falcon على عدة قضايا:

-يتم تحويل الرسالة (نصية، رقمية،...) المراد توقيعها إلى تمثيل عددي، مثلاً الرسالة BH تحول إلى (72 , 66)، ومن ثم يتم إيجاد كثير الحدود المعبر عنها: $m(x) = 66 + 72 x$

- يتم اختيار كثير حدود y(x) ، يُستخدم من أجل زيادة العشوائية في التوقيع بهدف منع الكشف عن المفتاح الخاص

-اختيار قيمة ملحية r (مجموعة بتات عشوائية) ، ويهدف إلى إمكانية توليد تواقيع مختلفة عند تطابق الرسائل.

-نحسب القيمة v : $v = y * h = 1 \mod q$

-نستخدم إحدى خوارزميات البصمة مثل SHA للحصول على البصمة الرقمية:

لـــ v مع السلسلة $(r \| m)$ أي $c = H(m , r , v)$

-نحسب $s(x) = r(x) + c(x)* f(x) \bmod q$ ، فيكون التوقيع هو (s,r)

٣- التحقق Verification من صحة التوقيع:

-نستخدم المفتاح العام في حساب $v' = s - c * h$

-نطبق خوارزمية الهاش لنحصل على c' : $\mathbf{c}' = H(m, r, v')$

-اذا كان $c = c'$ ، وكانت قيمة s ضمن الحدود المعينة للحجم عند ذلك يكون التوقيع صحيح .[8] [10].

ملاحظة: توجد عدة نسخ من Falcon، منها يستخدم معايير مختلفة قليلا بشكل لا يؤثر على المستوى الامني، (منها ما يتعلق بطول المفتاح و بالقيمة الملحية r، ومنها يتعلق بكثير الحدود العشوائي y ونقط اخرى تجعلها مختلفة قليلاً في سيناريو العمل) [8] .

الجدول رقم (٢) يلخص أطوال المفاتيح ، وصفة أزمنة التوليد، والتوقيع والتحقق من صحة التوقيع في هذه الخوارزمية

الجدول رقم (٢) المواصفات العامة لـ Falcon

المفتاح الخاص	١٢٨١ -٢٣٠٥ bytes
المفتاح العام	Falcon-512 (897)/ Falcon-1024 (1793) bytes
أكبر طول مفتاح	2305 bytes
أصغر طول مفتاح مقبول	1281 bytes
توليد المفاتيح	نسبياً بطيء
توقيت التوقيع	بطيء جداً
توقيت التحقق	نسبياً بطيء
حجم التوقيع	666 – 1280 bytes

نلاحظ من الجدولين ١ و ٢ أن خوارزمية ECC تتفوق على خوارزمية FALCON من حيث سرعة التوليد والتوقيع والتحقق وبطول توقيع أقل، ولكن لابد من دراسة هذه المعطيات من خلال التجريب على ملفات محددة (مختلفة بالحجم)، ولابد من دراسة ذلك وفقاً للمستويات الأمنية القياسية المعروفة وفي بيئات محددة.

النظم الهجينة Hybrid systems

نعلم أن الحواسيب التقليدية تعتمد على البتين (٠ أو ١) في عملها، ولكن الحواسيب الكمومية تعتمد على الكيوبت (qubits) الذي يمكن أن يكون في حالات متعددة في وقت واحد من خلال خاصية التراكب الكمومي، وهذا يسمح لهذه الحواسيب بالعمل بشكل أسرع بكثير مما هي عليه الآن، ولكن بنفس الوقت ظهرت للوجود الهجمات الكمومية، والتي تعتبر نوع من الهجمات التي تستغل قدرات الحوسبة الكمومية لكسر أمان الخوارزميات الكلاسيكية التي تستخدم حالياً في التشفير، من هنا نجد حتمية تطوير الآلية المستخدمة في حماية البيانات الرقمية من خلال استخدام النظم الهجينة Hybrid Systems القائمة على دمج أكثر من خوارزمية تشفير (تقليدية وكمومية) في نظام واحد [11].

المستويات الأمنية القياسية

اعتمدت في تقييم أداء الخوارزميتين على المستويات الأمنية القياسية المعتمدة من قبل المعهد الوطني للمعايير والتقنية (NIST) في الولايات المتحدة، والتي تم إقرارها واعتمادها عام ٢٠٠١، وفق مستويات أمان متعددة يوفرها المشفر القياسي العالمي AES.

- المستوى ١ : يعادل درجة أمان AES-128 و المستوى ٣ : والذي يعادل درجة أمان AES-١٩٢
- المستوى ٥ : يعادل درجة أمان عالي تحاكي أمان AES-256 [12].

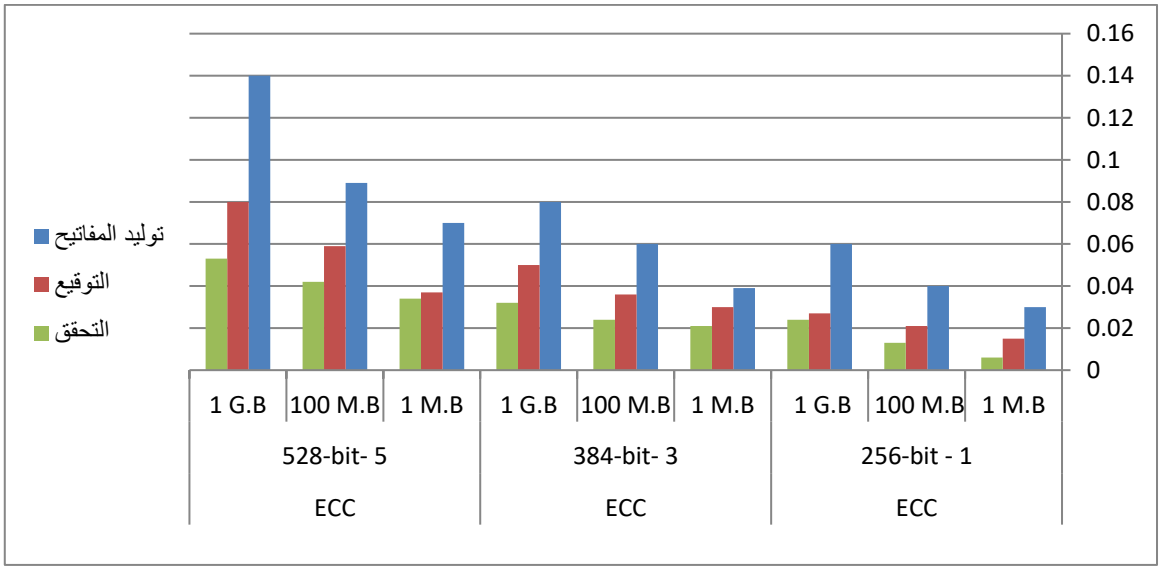
قمت في هذا البحث بإجراء تجارب متعددة واخذت المتوسط العام لنتائج هذه التجارب وذلك باستخدام حاسب بمعالج Intel Core i5، الذاكرة: ٨ جيجابايت، مع توفير المكتبات اللازمة مثل (OpenSSL ، PQClean)، واستخدمت ثلاث ملفات بأحجام مختلفة (ملفات بحجم ١ ميجابايت ، ١٠٠ ميجابايت، ١ جيجابايت) ، وذلك ضمن المستويات الأمنية الثلاث وفق ما تحتاجه الخوارزميات المدروسة من مفاتيح خاصة وعامة وبالأطوال المناسبة، ومن ثم حساب الأزمنة (بالثانية) اللازمة لتوليد المفاتيح، وزمن التوقيع، وزمن التحقق من صحة التوقيع، وتم اعتماد تنسيق (NIST) في تسمية هذه المستويات على الشكل[12] : ECC256-bit، ECC384-bit، ECC528-bit من أجل خوارزمية ECC، و Level 1, Level 2 , Level 3 من أجل خوارزمية Falcon، وحصلت على النتائج المبينة في الجدول رقم (٣) بالنسبة لخوارزمية ECC .

الجدول رقم (٣) النتائج الزمنية لـ ECDSA

الخوارزمية	المستوى	حجم الملف	توليد المفاتيح	التوقيع	التحقق
ECC	256-bit - 1	1 M.B	0.0٣	0.0١٥	0.00٦
		100 M.B	0.0٤	0.021	0.0١٣
		1 G.B	0.0٦	0.0٢7	0.0٢٤
ECC	384-bit- 3	1 M.B	0.039	0.0٣	0.0٢1
		100 M.B	0.0٦	0.03٦	0.0٢٤
		1 G.B	0.0٨	0.0٥	0.032
ECC	528-bit- 5	1 M.B	0.0٧	0.03٧	0.034
		100 M.B	0.089	0.059	0.042
		1 G.B	0.14	0.0٨	0.053

-نلاحظ أن خوارزمية ECC التي تعمل على المنحنيات الاهليليجية تنتقل من المستوى الأمني الأول وبطول مفتاح ٣٢ bytes إلى المستوى الأمني الثاني من خلال زيادة بسيطة على طول المفتاح ليصبح (48 bytes)، ثم إلى المستوى الثالث ، أيضاً من خلال زيادة بسيطة على طول المفتاح ليصبح (66 bytes).

-نلاحظ أيضاً استقرار في الأداء من خلال زيادات بسيطة في الزمن في المستويات الأمنية الثلاث ومن أجل الملفات المختلفة، رغم ارتفاع درجات الأمان من مستوى إلى أخر. يمكننا التعبير عن النتائج في الجدول رقم (٣) من خلال المخطط البياني رقم (١) الاتي:



الشكل رقم (١) النتائج الزمنية لـــ ECDSA

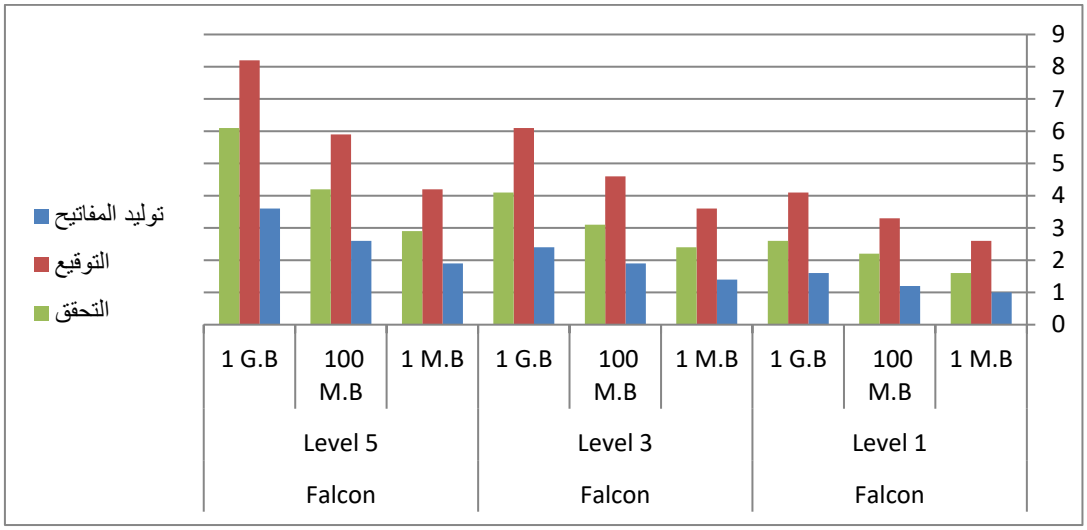
- تولد خوارزمية ECC مفاتيحها وتنتج التواقيع وتتحقق منها بأزمنة قليلة ومستقرة نسبيا في المستويات الأمنية المختلفة .
- بدراسة النتائج في الشكل رقم (١) السابق يتضح ان ECC تحتاج أزمنة متقاربة من أجل ملفات مختلفة الحجم ولاسيما في عملية التوقيع وذلك لأن التوقيع يتم على بصمة الملف وليس على بيانات الملف مباشرة.
- ايضاً نلاحظ ان عمليات التحقق من صحة التوقيع تتطلب زمن أقل مقارنة مع أزمنة توليد المفاتيح، وأزمنة إنتاج التواقيع .

اما بالنسبة لخوارزمية Falcon فإننا نقدم في الجدول رقم (٤) الآتي نتائج التنفيذ ضمن نفس الشروط السابقة من مواصفات الحاسب، وحجوم الملفات، وفي المستويات الأمنية الثلاث (أي من أجل طول المفتاح المناسب لكل مستوى أمني – ٨٩٧ ، ١٣٠٠ ، ١٧٩٣)، حيث الأزمنة مقاسة بالثانية ايضاً.

الجدول رقم (٤) النتائج الزمنية لـــ Falcon

الخوارزمية	المستوى	حجم الملف	توليد المفاتيح	التوقيع	التحقق
Falcon	Level 1	1 M.B	1.0	٢.٦	١.٦
		100 M.B	.١2	٣.٣	٢.٢
		1 G.B	.١6	٤.١	٢.٦
Falcon	Level 2	1 M.B	.١4	٣.٦	٢.٤
		100 M.B	.١9	٤.٦	٣.١
		1 G.B	.٢4	٦.١	٤.١
Falcon	Level 3	1 M.B	.١9	٤.٢	٢.٩
		100 M.B	.٢6	٥.٩	٤.٢
		1 G.B	3.6	8.٢	6.١

يمكننا التعبير عن النتائج في الجدول رقم (٤) من خلال المخطط البياني رقم (٢) الاتي:



الشكل رقم (٢) النتائج الزمنية لـــ Falcon

-بدراسة الشكل رقم (٢) السابق نلاحظ ان خوارزمية Falcon تحتاج زمناً أطول بشكل كبير يتراوح بين عشرات الاضعاف إلى المئات، وذلك بسبب تعقيد العمليات التي تحتاجها، ففي عملية التوليد يرتفع الزمن إلى حوالي 29 ضعف، بينما في عملية التوقيع فإن Falcon تحتاج إلى أكثر من ١٢٠ ضعف، وفي مجال التحقق من صحة التوقيع يزداد الزمن إلى أكثر من ١١٧ ضعف.

-كما أن الانتقال من مستوى أمني إلى مستوى أمني أعلى يتطلب زيادة كبيرة في أطوال المفاتيح العامة والخاصة.

من المهم أن نعلم أن خوارزمية Falcon تستهلك طاقة وموارد تصل إلى أكثر من ٢٠ ضعف من خوارزمية، ويكون ذلك بشكل عام ، ولكن بالخصوص أثناء عملية التوقيع ترتفع أكثر من ذلك بسبب تعقيد العمليات التي تستخدمها [13][14]، نبين استهلاك كل من الخوارزميتين للطاقة مقاسة بالميلي جول m j في المستويين الأول والخامس وفي نفس بيئة المقارنة السابقة (معالج i5 وذاكرة ٨ جيجابايت) في الجدول رقم (٥) الآتي [15] :

الجدول رقم (٥) يبين استهلاك الطاقة في الخوارزميتين

الخوارزمية	المستوى	توليد المفاتيح	التوقيع	التحقق
ECC-256	AES-128	15 mJ	7 Mj	10 mJ
ECC-528	AES-256	25 – 35 mJ	20 – 28 mJ	25 – 30 mJ
Falcon-512	AES-128	350 mJ	300 mJ	200 mJ
Falcon-1024	AES-256	500-600 mJ	400-500 mJ	300-400 mJ

نلاحظ من الجدول رقم (٥) السابق، أن الحاجة للطاقة في المستوى الأمني الأول بالنسبة لخوارزمية ECC بسيط، وفي المستوى الأمني الخامس أيضاً يبقى بسيط وهذا سيكون مناسب للأجهزة منخفضة الاستهلاك للطاقة (مثل الهواتف الذكية، وإنترنت الاشياءIoT) [16]، ولكن بالنسبة لخوارزمية Falcon فالحاجة للطاقة كبير في المستوى الأول وكبير جداً في المستوى الخامس، وهذا يشكل مشكلة في البيئات مجدودة الطاقة أو الموارد، كذلك بالنسبة لاستهلاك الذاكرة والمعالج، فإن خوارزمية Falcon تستهلك منها أكثر من ١٥ ضعف مما تستهلكه خوارزمية ECC، وذلك في المستويات الأمنية المختلفة [17] .

التنفيذ في بيئات أخرى

قمنا بتنفيذ الخوارزميتين في المستويات الأمنية الثلاث على حاسب i7 ومع ذاكرة ١٦ جيجابايت، ووجدنا تحسن كبير في أداء الخوارزميتين، ويعود سبب ذلك لعدد النوى التي يوفرها والتردد الأعلى و المعالجة المتوازية مما يسمح بتوزيع العمل بكفاءة أكبر عما هي عليه على حاسب i5 مع ذاكرة ٨ جيجابايت، ولكن وجدنا تشعب في موضوع التنفيذ والتحسن وفقا لمعطيات أخرى ومنها استخدام المكتبات المناسبة، والعمل وفق multithreaded أو single-threaded، وبالمحصلة وجدنا تحسن كبير في أزمنة توليد المفاتيح، وزمن التوقيع والتحقق كما هو مبين بالجدولين رقم (٦) و (٧) الآتيين:

الجدول رقم (٦) الأزمنة اللازمة في خوارزمية ECC

الخوارزمية	المستوى	حجم الملف	توليد المفاتيح	التوقيع	زمن التحقق
ECC	256-bit - 1	1 M.B	0.02	0.008	0.004
		100 M.B	0.021	0.009	0.005
		1 G.B	0.032	0.014	0.007
ECC	384-bit- 3	1 M.B	0.021	0.013	0.006
		100 M.B	0.026	0.018	0.007
		1 G.B	0.034	0.024	0.014
ECC	528-bit- 5	1 M.B	0.036	0.02	0.014
		100 M.B	0.041	0.028	0.018
		1 G.B	0.052	0.034	0.023

بإجراء دراسة مقارنة للجدولين رقم ٣ و رقم ٦ نجد نسبة متوسط التحسين في مجال توليد المفاتيح في ECC أكثر من 50% ، أما نسبة متوسط التحسين في مجال التوقيع تتجاوز 52%، وفي مجال التحقق من صحة التوقيع فتتجاوز 60% .

الجدول رقم (٧) الأزمنة اللازمة في خوارزمية Falcon

الخوارزمية	المستوى	حجم الملف	توليد المفاتيح	التوقيع	زمن التحقق
Falcon	Level 1	1 M.B	0.8	1.7	1.2
		100 M.B	1.0	2.2	1.5
		1 G.B	1.4	3.2	2.2
Falcon	Level 2	1 M.B	1.2	2.6	1.8
		100 M.B	1.5	3.7	2.7
		1 G.B	2.0	5.2	4.0
Falcon	Level 5	1 M.B	1.7	3.8	2.7
		100 M.B	2.3	5.2	4.1
		1 G.B	3.0	7.7	6.2

بإجراء دراسة مقارنة للجدولين رقم ٤ و رقم ٧ نجد نسبة متوسط التحسين في مجال توليد المفاتيح في Falcon أكثر من 15%، أما نسبة متوسط التحسين في مجال التوقيع تتجاوز 17%، وفي مجال التحقق من صحة التوقيع فتتجاوز 10%.

وبدراسة الجدولين رقم ٦ ورقم ٧، نلاحظ ازدياد الفوارق عند الانتقال إلى بيئة i7، حيث في التوليد تبقى خوارزمية ECC أسرع وبمقدر ٥٠ ضعف، و في التوقيع أيضاً ECC اسرع بمقدار ٢١٤ ضعف، أما في التحقق فتصل إلى أكثر من ٢٧٠ ضعف.

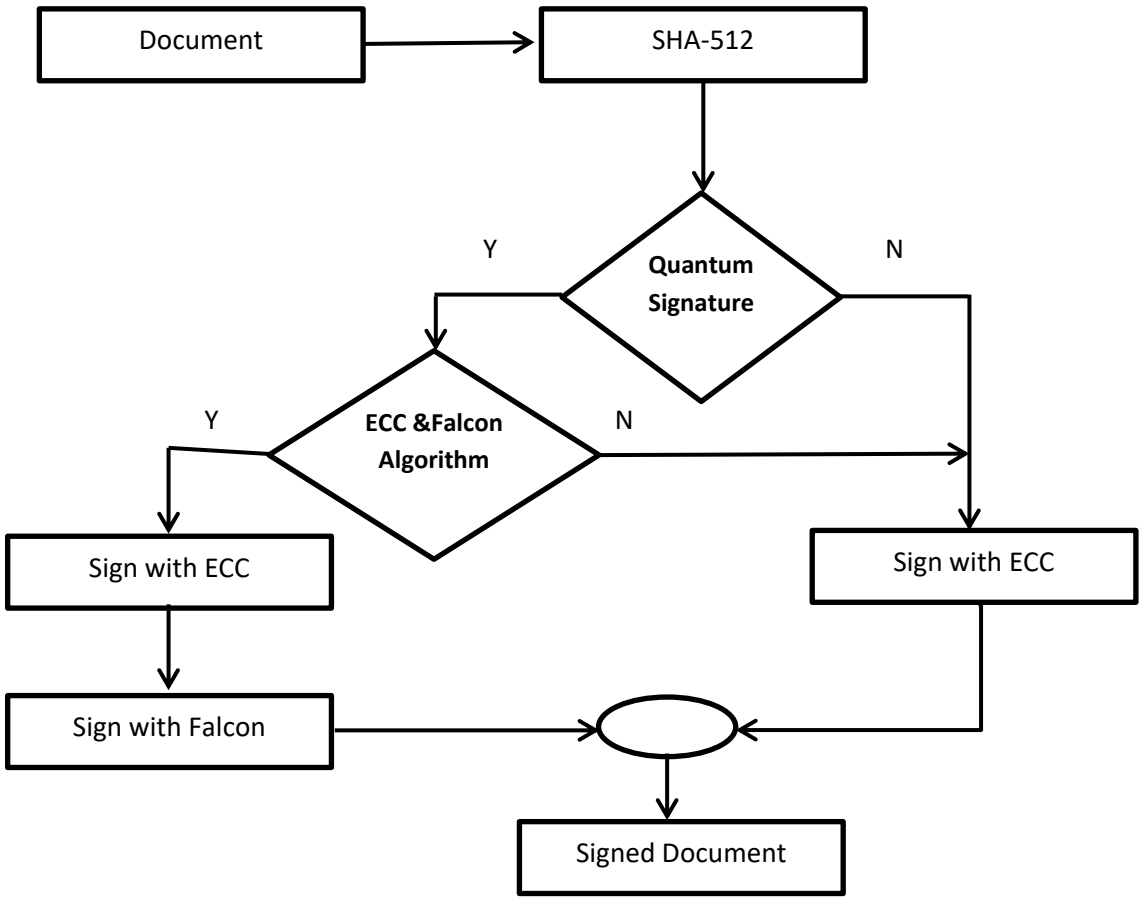
ورافق ذلك تحسن في استهلاك الطاقة بسبب سرعة المعالج مما يقلل زمن التشغيل، حيث انخفض استهلاك الطاقة في المستوى الأول بالنسبة لخوارزمية ECC إلى 10,5 mj بدلاً من 15 mj في التوليد، ومن ٧ إلى 4.9 في التوقيع، ومن ١٠ إلى7 أي بنسبة تحسين تصل إلى 30%، وفي خوارزمية Falcon أيضاً انخفض من ٣٥٠ ميلي جول إلى ٢٤٥ ميلي جول، وفي التوقيع من 300 mj إلى 210 mj ، وفي التحقق من 200 mj إلى 140 mj أي بنسبة تحسن عامة 30% ، ولكن النتيجة الأهم بالموضوع كانت بالمحافظة على الفوارق النسبية بين أداء الخوارزميتين في المستوى الأمنية [18] [17] .

النظام الهجين المقترح:

على الرغم مما تتمتع به خوارزمية ECC من سرعة وأمان ودقة فإنها لن تكون قادرة على مواكبة الإمكانيات الكبيرة للحوسبة الكمومية، ولاحظنا أيضاً أن خوارزمية Falcon رغم ما توفره من مستوى أمني عالي وإمكانيات العمل على التوازي [19]، كما انها تستطيع ان تعطي تواقيع صغيرة الحجم واستهلاك متوسط للذاكرة مقارنةً مع خوارزميات كمومية اخرى، ولكنها بالمقارنة مع خوارزمية ECC أبطأ وتحتاج مفاتيح طويلة وتُنتج تواقيع طويلة وهذا غير مناسب للعمل ولاسيما في البيئات الحالية [1][13].

نقترح الابقاء على خوارزمية ECC ولاسيما في البيئات الحالية والبيئات المحدودة الموارد، والعمل على الاستفادة من الامكانيات التي توفرها في البيئات المستقبلية ولاسيما في تبادل مفاتيح الجلسة، حيث يتم دمجها مع خوارزميات ما بعد الكم (Post- Quantum) في نفس النظام، ولاسيما انها أظهرت تحسنا وتوازنا في الأداء ومستوى الأمان من خلال تقسيم التوقيعات الكبيرة إلى أجزاء أصغر عند إرسالها عبر الشبكة، حيث تم استخدامها ضمن تقنية سلاسل الكتل Blockchains، و بشكل هجين في انترنت الاشياء [20] [16].

يقوم النظام الهجين المقترح على دمج خوارزمية ECC مع خوارزمية Falcon كما هو موضح في الشكل رقم (٣)، وذلك من أجل الاستفادة من سرعة اداء ECC وحاجتها البسيطة من الموارد، إضافة إلى تحقيق مستويات أمنية عالية في البيئات الحالية، والوقوف في وجه الهجمات الكمومية المستقبلية من خلال خوارزمية Falcon، ولاسيما ان العديد من المنصات والبروتوكولات الحالية تعتمد في تحقيق سلامة البيانات وإثبات مصدرها على خوارزمية ECC وحيث أن عملية الانتقال الكامل لخوارزميات ما بعد الكم (PQC)سيحتاج لوقت طويل نسبياً ويتطلب توفر الحواسيب الكمومية بصيغتها التجارية، ويمكننا هذا النظام المقترح من إضافة خوارزميات كمومية بطريقة موازية دون انقطاع الخدمات، ويتيح لنا إجراء توقعين على الوثيقة والحصول على درجة أمان مضاعفة من خلال استخدام مفتاحين من أجل الخوارزميتين , ECC Falcon، ويتمتع النظام الهجين المقترح ببنية أساسية تدعم كل من ECC و Falcon، ويمكننا من استغلال سرعة اداء ECC في جلسة الاتصال لتبادل المفاتيح بشكل سريع جداً، ويسمح بتخصيص خوارزمية ECC للبيئات التي تحتاج السرعة وقلة الموارد، وتخصيص الخوارزمية الكمومية Falcon للعملاء المستعدين لاستخدام التوقيع الكمومي أو التوقيع الهجين، وهذا ضروري جداً إلى حين نضوج التقنيات الكمومية، مما يوفر مرونة تناسب البيئات المختلفة، وأمان طويل الأمد يحمي البيانات من أقوى الهجمات، ويؤمن توافقية كمومية مع النظم الأمنية الحالية دون تغييرها كلياً، أما بالنسبة لزيادة التكلفة الحسابية فلن تسبب مشكلة في عالم الكم وتقنياته المنتظرة.



الشكل رقم (٣) مخطط للنظام الهجين المقترح

النتائج

قمنا في هذا البحث [illegible] شاملة تجمع بين التحليل النظري والعملي للخوارزمية المعتمدة على المنحنيات الاهليليجية ECC، ونظام التوقيع الرقمي الكمومي باستخدام خوارزمية Falcon، وشملت الدراسة مقارنة بنيوية دقيقة بين النظامين من حيث المفاهيم الرياضية، البنية الأمنية، وطريقة توليد المفاتيح والتوقيع والتحقق من صحة التوقيع، بالإضافة لمقارنة المتطلبات التشغيلية لكل من النظامين، ولاسيما مستوى الحاجة للطاقة والموارد، كما أجرينا دراسة تحليلية للنتائج التنفيذية للخوارزميتين في بيئتين وعلى ملفات مختلفة الحجوم، وفي المستويات الأمنية القياسية المعتمدة، وخلصت الدراسة بالنهاية إلى النتائج الآتية:

١- سرعة توليد المفاتيح في خوارزمية ECC تزيد عن خوارزمية Falcon بالمتوسط (في البيئتين i5 , i7) إلى أكثر من ٣٥ ضعف، أما في التوقيع فتزيد السرعة في خوارزمية ECC إلى أكثر من ١٦٧ ضعف عنها في خوارزمية Falcon، كما أن سرعة التحقق من صحة التوقيع في خوارزمية ECC تزيد بحوالي ١٦٥ ضعف.

٢- في مجال استهلاك الطاقة فإن خوارزمية Falcon تحتاج إلى ٣٥٠ ميلي جول لتوليد المفاتيح مقابل ١٥ ميلي جول في خوارزمية ECC، وفي التوقيع تحتاج خوارزمية Falcon من ٤٠٠ ميلي جول مقابل ٢٠ في ECC، أما في التحقق فإن Falcon تحتاج ٢٠٠ ميلي جول في حين تحتاج ECC إلى ١٠ ميلي جول، وهذا يُظهر أهمية استخدام ECC في البيئات المحدودة الموارد وعدم إمكانية استخدام Falcon.

٣- بالنسبة للبيئات الحالية التي لا تعتمد على تكنولوجيا الكم، تتميز خوارزمية ECC بأدائها المميز من حيث السرعة وكفاءة استخدام الموارد، بالإضافة إلى مستويات الأمان العالية التي توفرها مع إمكانية تعزيز مستوى الأمان فيها من خلال زيادة طول المفاتيح المستخدمة، حيث أن هذه الزيادة لا تؤثر بشكل كبير على سرعة الأداء أو استهلاك الموارد، وهذا يجعل ECC خياراً مرناً قابلاً للتطوير في ظل الظروف الحالية وحتى فترة انتقالية قبل الاعتماد الكامل على تقنيات ما بعد الكم، إضافة إلى فاعليها العالية الحالية والمستقبلية في عملية تبادل المفاتيح.

٤- ان النظام الهجين المقترح الذي يجمع بين ECC و Falcon يتمتع ببنية تصميمية مرنة تسمح بالاستخدام المدمج أو المنفصل للخوارزميتين وذلك حسب المتطلبات ومقتضيات بيئة العمل، ويوفر أداء عالي وفاعلية أمنية مناسبة للبيئات الحالية والمستقبلية.

التوصيات

١- توصي الدراسة بضرورة الاعتماد حالياً وفي المستقبل القريب على خوارزمية ECC، ولاسيما بعد تحسين مستويات الأمان الخاصة بها من خلال زيادة أطوال المفاتيح المستخدمة، و إتباع استراتيجيات أمنية مستقبلية في مجال سلامة الوثائق الرقمية وإثبات الهوية بحيث يتم الاستفادة من نقاط القوة لدى خوارزميات الجيل الحالي، وجيل الخوارزميات الكمومية في إنتاج التواقيع الرقمية في البيئة الكمومية، وذلك من خلال الاعتماد على النظام الهجين المقترح، وعلى نظم هجينة مشابهة ومناسبة لمختلف بيئات العمل وقادرة على الوقوف في وجه الهجمات الكمومية المستقبلية .

٢- العمل على تطوير أنظمة تشفير هجينة اعتماداً على خوارزميات كمومية اخرى بالتشارك مع خوارزمية الجيل الحالي .

المراجع

1. P. Gajland, J. Janneck, E. Kiltz,*" A Closer Look at Falcon*" , Ruhr University Bochum,2025.
2. J. Goertzen, D. Stebila, "*Post-Quantum Signatures in DNSSEC via Request-Based Fragmentation*", University of Waterloo, 2022.
٣. برهوم، بسيم ، *"تصميم وبناء بروتوكول أمني لحماية الوثائق الرقمية"*، مجلة جامعة طرطوس، المجلد الخامس، ٢٠٢١.
4. M. Zubaidie, Z. Zhang,J.Zhang, *" Efficient and Secure ECDSA Algorithm and its Applications: A Survey*", University of Southern Queensland, Australia, 2019.
5. M. Smith, J. Lee, "*Comparative Analysis of ECC and Lattice-Based Cryptography for Energy Efficiency*" , Journal of Cryptographic Engineering, 2022.
6. H. Wang, Y. Liu, "*Elliptic Curve Cryptography: Principles and Applications in the Quantum Era"* , IEEE Transactions on Information Forensics and Security, 2023.

7. A. Banerjee ,U. Banerjee, "*A High-Performance Curve25519 and Curve448 Unified Elliptic Curve Cryptography Accelerator*", Indian Institute of Science,2025.

8. D. Stehlé, R. Steinfeld, *"Falcon: Fast-Fourier Lattice-Based Compact Signatures on the NIST PQC Standardization Process*", *Conference:* PQCrypto ,2021.

9. A.Lakhan, *" A Comparative Study On Post-Quantum Cryptographic Digital Signature Algorithms*",Carleton University Ottawa , 2023.

10. T. Prest, P.Alain Fouque, T. Güneysu, et al ,"*Falcon: Fast Fourier Lattice-based Compact Signatures over NTRU",* Journal of Cryptology, 2021.

11. M. Rossi, L. Valli, F. Simula ,*"Hybrid Cryptographic Schemes for Quantum-Resistant Communications in IoT",* IEEE Communications Surveys & Tutorials, 2023.

12. N. Chiano, R. Longo, A. Meneghetti, G. Santilli, "*A survey on NIST PQ signatures",* University of Trento,2021.

13. L. Chen, K. Zhao, "*Post-Quantum Cryptography: Falcon vs ECC in Resource-Constrained Environments*", *Conference:* ACM CCS Workshop, 2023.

14. A. Fernandez, R. Gupta, "*Implementing ECC and Falcon on FPGA: Resource Utilization and Power Consumption*",International Symposium on Hardware Security, 2022.

15. K. Morozov, D. Rossi , "*Elliptic Curves vs. Lattice-Based Schemes: Security and Efficiency in the Quantum Computing Era*", ACM Computing Surveys, 2023.

16. J. Ntayagabiri, J. Ndikumagenge, Y. Bentaleb, H. Makhtoum, *"Comparative Analysis of Elliptic Curve-Based Cryptographic Approaches for Internet of Things Security*", International Journal of Scientific Research in Computer Science,2024.

17. P. Novak, T. Chen ,"*Energy Analysis of Falcon Signature Scheme on Embedded Systems*" , IEEE Access, 2024.

18. N. Luc, T. Nguyen, D. Quach, T. Dao, N. Pham, " *Building Applications and Developing Digital Signature Devices based on the Falcon Post-Quantum Digital Signature Scheme"*, Engineering, Technology & Applied Science Research,2023.

19. W. Li, H. Wei, S. Shen, H.Yang, W.Dai, Y. Zhao, *" cuFalcon: An Adaptive Parallel GPU Implementation for High-Performance Falcon Acceleration",* JOURNAL OF LATEX CLASS FILES, 2024.

20. Z.Yang, H, Alfauri , B. Farkiani , R.Jain, R. Pietro, A. Erbad, *"A Survey and Comparison of Post-Quantum and Quantum Blockchains",* IEEE communications surveys & tutorials, 2024.