تقييم أداء خوارزمية التشفير غير المتناظر (MQQ- ENC) في شبكات الحساسات اللاسلكية الداعمة للوسائط المتعددة

د. بشرى معلا•

خديجة اسكندر ••

(تاريخ الإيداع 21 / 12 / 2020. قُبِل للنشر في 1/ 7 / 2021)

□ ملخّص □

تتكون شبكة الحساسات اللاسلكية الداعمة للوسائط المتعددة (WMSN) من عدد كبير من العقد الحساسة صغيرة الحجم، منخفضة الطاقة، ومحدودة الموارد، تنشر في حقل الاختبار. تمتلك هذه العقد القدرة على تحسس معطيات الوسائط المتعددة من البيئة المحيطة، وتخزينها، ومعالجتها وإرسالها في الزمن الحقيقي. تُعدّ قضية الأمن في هذه الشبكات إحدى القضايا المهمّة للدراسة، وذلك نظراً لطبيعتها الخاصّة، إضافة إلى أهمية تحقيق متطلبات الأمن الأساسية للمعلومات المُرسَلة عبر الشبكة. يُعدّ استخدام تقنيات التشفير من الأساليب الفعالة لتحقيق متطلبات الأمن الأساسية في هذه الشبكة. إنَ خوارزمية MQQ التي اقترحت حديثاً، هي إحدى خوارزميات المفتاح العام PKC، والتي حققت هذه الخوارزمية أداءً جيّداً مقارنةً مع نظيراتها من خوارزميات المفتاح العام الأخرى.

نقدّم في هذا البحث دراسة تحليلية لتطبيق خوارزمية التشفير غير المتناظر MQQ في شبكات الحساسات اللاسلكية الداعمة للوسائط المتعددة. لتحقيق هدفنا استخدمنا صوراً حقيقية ملتقطة من قبل عقدة حساس لاسلكي داعم للوسائط المتعددة، وتم دراسة بعض البارامترات الهامّة التي تقيم أداء هذه الخوارزمية مثل حجم المفاتيح المولدة والصور المشفرة، وزمن التنفيذ، والحيز المحجوز من ذاكرة الحساس، إضافة إلى درجة تعقيد الخوارزمية المدروسة.

أظهرت النتائج أن خوارزمية MQQ-ENC قدمت أداءً جيداً، إذ أن زمن تنفيذ العمليات أفضل مما هو عليه في خوارزمية RSA. كما بينت النتائج أيضاً ضرورة أخذ الحجم الكبير للمفتاح العام بالحسبان عند تطبيقها في شبكات الحساسات اللاسلكية الداعمة للوسائط المتعددة.

الكلمات المفتاحية: شبكات الحساسات اللاسلكية الداعمة للوسائط المتعددة، خوارزمية المفتاح العام، التشفير، أشباه الزمر، خوارزمية المفتاح العام المعتمدة على أشباه الزّمر التربيعية.

• أستاذ مساعد، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سورية. boushra.maala@gmail.com

•• قائم بالأعمال، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سورية. Kh.eskndar.1991@hotmail.com

Performance Evaluation of Asymmetric Encryption Algorithm (MQQ-ENC) in Wireless Multimedia Sensor Networks

Dr. Boushra Maala*
Khadijeh Iskander**

(Received 21 / 12 / 2020. Accepted 1 / 7 / 2021)

□ ABSTRACT □

Wireless Multimedia Sensor Network (WMSN) consists of a large number of small size, low power, limited sources sensor nodes, deployed in tested field, These nodes have the ability of sensing, processing, storing and sending multimedia data from the tested field in real time. The security in WMSNs is one of most important issues that should be studied due to the special nature of this network, and of the importance of inquest basic security requirements when sending information in the network. Using cryptography technics are very effective ways to realize basic security requirements in this network. The recently proposed MQQ algorithm is one of public key cryptography (PKC) algorithms, which provides a good performance compared to other PKC algorithms.

In this research, we present an analyzing study of MQQ implementation in WMSNs. To achieve our goal, we used real images taken by multimedia wireless sensor nodes. We studied the most important parameters such as the size of generated keys and encrypted images, the execution time and the space occupied in the flash memory of multimedia wireless sensor nodes and complexity degree of this algorithm.

Results showed that MQQ has good performance, as well as the execution time of operations is better than RSA algorithm. Results also showed the importance of taking into account a large size of public key of MQQ algorithm when implementation it in WMSNs.

Keywords: wireless multimedia sensor networks, public key cryptography, encryption, quasi-groups, Multivariate Quadratic Quasi groups cryptography algorithm.

* **Associate Professor, Department of Communication and Electronics, Factually of Mechanical and Electrical Engineering, Tishreen University, Lattakia, Syria. boushra.maala@gmail.com**
** **Academic Assistant, Department of Communication and Electronics, Factually of Mechanical and Electrical Engineering, Tishreen University, Lattakia, Syria. Kh.eskndar.1991@hotmail.com**

مقدّمة:

جاءت شبكات الحساسات اللاسلكية الداعمة للوسائط المتعددة WMSNs (Wireless Multimedia Sensor Networks) كتطورٍ منطقي لشبكات الحساسات اللاسلكية التقليدية Traditional Scalar Wireless Sensor Networks، وتوجهت الكثير من الأبحاث الحديثة نحو دراسة شبكات الحساسات اللاسلكية الداعمة للوسائط المتعددة، ويعزى ذلك ببساطة إلى غنى التطبيقات التي تقدمها هذه الشبكات، وإلى توجهها نحو مختلف المجالات بدءاً بالتطبيقات الطبية إلى الاتصالات الفضائية مروراً بالتطبيقات البيئية والخدمية والصناعية والعسكرية، وغيرها. تتكون هذه الشبكات من عدد من الحساسات صغيرة الحجم وذاتية التغذية، مزودة بتجهيزات خاصة كالكاميرات والمايكروفونات تمكنها من التقاط معلومات الوسائط المتعددة، كالصوت والصور والفيديو، والخاصة بظاهرة ما في الوسط المحيط، ثم تنقل هذه المعلومات لاسلكياً إلى المحطة الرئيسية للاستفادة منها، ومن ثمّ تقوم المحطة الرئيسية بإيصال المعلومات إلى المستخدم عبر الإنترنت أو الأقمار الصناعية [1,2].

مع هذا الانتشار الواسع لهذه الشبكات وتنوّع تطبيقاتها، تظهر التحديات الأمنية انطلاقاً من الطبيعة الخاصة لهذه الشبكات، كطبيعة المنطقة التي تنشر فيها الحساسات والتي قد يكون من الصعب مراقبتها مباشرة، والطبيعة الفيزيائية للحساسات (سريعة الفشل، غير مقاومة للتلاعب)، والطبولوجيا غير الثابتة (إضافة وإزالة عقد حساسة)، إضافة إلى الثغرات الأمنية الناتجة عن الاتصالات اللاسلكية. لذلك فإن البيانات المرسلة عبر الشبكة يمكن أن تتعرّض للعديد من الاختراقات الأمنية كالتنصّت والتزييف وتعديل محتوى الرسالة، لذلك كان هناك الكثير من الدراسات والأبحاث حول قضايا الأمن في هذه الشبكات، ووُضعت العديد من الإجرائيات والمخططات الأمنية وخوارزميات التشفير لتوفير الحماية لمعلومات الشبكة، ومقاومة الاختراقات الأمنية. يُعدّ استخدام تقنيات التشفير من أكثر الأساليب الأمنية الفعالة لتحقيق متطلبات الأمن الأساسية للبيانات المنقولة عبر الشبكة [3,4] .

ظهرت مؤخّراً خوارزمية المفتاح العام MQQ (Multivariate Quadratic Quasigroup)، وهي إحدى خوارزميات المفتاح العام المعتمدة على كثيرات الحدود التربيعية متعددة المتحوّلات MQPKC (Multivariate Quadratic Public Key Cryptosystems)، وتميّز هذا النوع من الخوارزميات بتحقيقه أداءً جيّداً مقارنة مع خوارزميات المفتاح العام الأخرى [5].

أهمية البحث وأهدافه:

يُعد تحقيق متطلبات الأمن الأساسية في شبكات الـ WMSNs أمراً مهمّاً، وذلك لكون المعلومات التي تُرسل عبر هذه الشبكات كتدفقات الفيديو والصوت والصور تتطلب في كثير من التطبيقات مستوى عالٍ من السرية والتكاملية والمصادقة. كما أنّ طبيعة هذه الشبكات وطريقة نشر العقد الحساسة وطبيعة الاتصال اللاسلكي، كل ذلك يجعل اختراق هذه الشبكات وتهديد أمنها أمراً ممكناً. ولحماية بيانات الشبكة من التنصت والتعديل والتزييف كان هناك حاجة لاستخدام تقنيات التشفير.

يهدف هذا البحث إلى 1- التعرّف على خوارزمية المفتاح العام MQQ وبارامتراتها، 2- دراسة تحليلية لتطبيق خوارزمية التشفير MQQ-ENC في شبكات الـ WMSNs ، 3- تقييم أداء هذه الخوارزمية من خلال مقارنتها مع خوارزمية المفتاح العام RSA الشهيرة.

طرائق البحث ومواده:

برمجت جميع مراحل خوارزمية MQQ بلغة C [6]، ونفذت وطبقت باستخدام برنامج (Code::Blocks /version 16.01)، وهو عبارة عن مترجم خاص بلغة (C/C++).

من أجل عمليتي التشفير وفك التشفير صممنا واجهة باستخدام بيئة visual studio 2015 community edition وهو برنامج مجّاني حمَّل من موقع Microsoft [7] وبرمجت الواجهة بلغة C #. ثم حولنا ملفات الـ MQQ الخاصة بتوليد المفاتيح والتشفير وفك التشفير(البرامج بلغة C) إلى مكتبة dynamic link library(dll) عن طريق برنامج الـ code blocks. ومن ثم استخدامنا مكتبة dll عن طريق C# ، وبهذه الطريقة ربطت الواجهة مع أكواد الـ MQQ ، ومن أجل قياس زمن التنفيذ بشكل دقيق استخدمنا الصنف ( )stopwatch .

تمت المقارنة مع خوارزمية المفتاح العام RSA مكتوبة بلغة البرمجة C والمضمنة في مكتبة openssl [8]، وهي عبارة عن مكتبة مفتوحة المصدر تحتوي على أدوات التشفير وتستعمل بروتوكولات طبقة النقل الآمن، و هي تنفذ المهام الأساسية للتشفير وتوفر وظائف مختلفة. يمكن استخدام openssl في مجموعة متنوعة من لغات البرمجة، و إصدارات متاحة لمعظم أنظمة التشغيل. نفذت مراحل خوارزمية RSA (توليد المفاتيح، التشفير، فك التشفير) باستخدام برنامج win32openssl [9]، وهو عبارة عن تطبيق لهذه المكتبة يعمل على أنظمة windows.

1. الدراسة المرجعية:

اعتمدت الكثير من بروتوكولات الأمن في هذه الشبكات على خوارزميات المفتاح العام PKC لفعاليتها في الحفاظ على سرية المعلومات كونها تعتمد على زوج من المفاتيح(عام وخاص)، ومن أشهرها خوارزمية DH (Diffie – Hellman) التي تعتمد على صعوبة حل اللوغاريتمات المتقطعة، وقد استخدمت كخوارزمية لتبادل المفاتيح بين الأطراف المتصلة. وخوارزمية RSA (Rivest,Shamir and Adleman) والتي تعتمد على صعوبة تحليل أعداد صحيحة كبيرة إلى عواملها الأولية. إضافة إلى خوارزمية ECC (Elliptic Curve Cryptography) المبنية على مسألة لوغاريتمات متقطعة تنجز تبادل مفتاح Diffie-Hellman وغيره عن طريق منحنيات القطع الناقص. حققت هذه الخوارزميات الشائعة مستوى أمن عال، إلّا أنها تمتلك نقطة ضعف أساسية هي سرعتها المنخفضة، واعتمادها على توابع رياضية معقدة تتطلب قدرات حسابية ومعالجة عالية، وهذا بدوره يستهلك الكثير من موارد الشبكة المحدودة [10,11,12].

ظهرت في منتصف الثمانينات خوارزميات المفتاح العام المعتمدة على كثيرات حدود من الدرجة الثانية ومتعددة المتحولات MQPKC (Multivariate Quadratic PKC)، كبديل لخوارزميات التشفير بالمفتاح العام التقليدية(RSA,ECC) التي تعتمد في مبدأ عملها على توابع رياضية معقدة وصعبة الحل. وكان الدافع الأساسي هو: "إيجاد مخطط تشفير غير متناظر يحقق متطلبات الأمن ويمتلك أفضل سرعة"، وكان من أهمّ أصنافها خوارزمية MQQ التي تعتمد على أشباه الزّمر. تميّز هذا الصنف من خوارزميات المفتاح العام بسرعته العالية في عمليتي التشفير وفك التشفير، إضافة إلى سرعته في توليد التواقيع الرقمية والتحقق منها، وتميزت باعتمادها على عمليات رياضية بسيطة، كما أنها أكثر مرونة من الخوارزميات السابقة، إذ أنها بقيت آمنة وفعالة بالرغم من التطور الكبير في قدرات المعالجة للحواسيب [5,13,14,15].

وفيما يأتي سنقدم دراسة مرجعية تفصيلية للنقاط التي يعتمد عليها بحثنا.

1.1 التشفير Encryption:

يعرَّف التشفير بأنَّه عملية تحويل المعلومات إلى شفرات غير مفهومة لمنع الأشخاص غير المرخَّص لهم من الاطلاع على المعلومات أو فهمها، وذلك اعتماداً على خوارزمية معينة وباستخدام مفاتيح محددة في تشفير الرسالة وفك تشفيرها. تستند هذه المفاتيح إلى صيغ رياضية وخوارزميات معقّدة، وتعتمد قوّة وفعاليّة التشفير على عاملين أساسيين هما: الخوارزمية المستخدمة، و طول المفتاح رقمياً (مقدراً بالبت).

ومن ناحية أخرى فإن فك التشفير هو عمليّة إعادة تحويل البيانات المُشَفّرَة إلى صيغتها الأصليّة، وذلك باستخدام المفتاح المناسب لفك الشيفرة [10].

تقسم خوارزميات التشفير تبعاً للمفاتيح المستخدمة في عمليتي التشفير وفك التشفير إلى خوارزميات تشفير متناظر وخوارزميات تشفير غير متناظر.

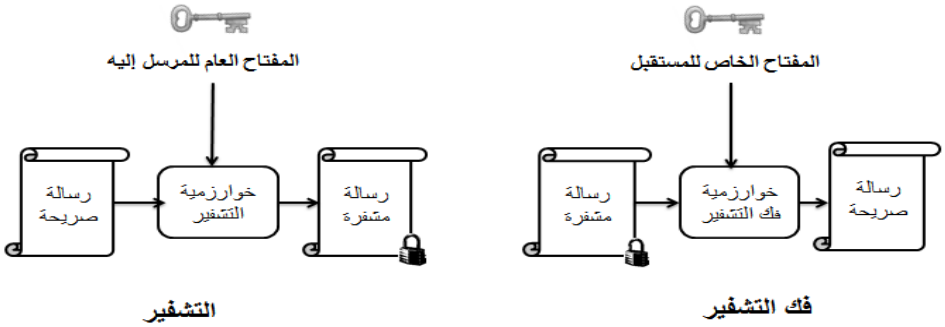
في خوارزميّة التشفير المتناظر: يستخدم مفتاح سري مشترك بين المرسل والمستقبل للتشفير وفك التشفير.

في خوارزميّة التشفير غير المتناظر : يستخدم زوج من المفاتيح، مفتاح عام (Public Key) للتشفير ومفتاح خاص (Private Key) لفك التشفير. إنّ الاسم الأكثر شيوعاً لخوارزميّة التشفير غير المتناظر هو خوارزمية المفتاح العام PKC(Public Key Cryptography).

– يكون المفتاح العام لعقدة ما ضمن الشبكة معروفاً من قبل جميع عقد هذه الشبكة ويستخدم من قبل أي منها لتشفير الرسائل المرسلة إلى صاحب هذا المفتاح، بينما يبقى المفتاح الخاص سراً لدى العقدة فقط حيث يكون معلوماً من قبلها فقط. يستخدم المفتاح الخاص لفك تشفير الرسائل التي تمَّ تشفيرها بالمفتاح العام المقابل له، كما هو مبين بالشكل (1).

عموماً تُعدّ خوارزميات التشفير غير المتناظر أكثر أماناً من خوارزميات التشفير المتناظر، حيث أنه في حال معرفة مفتاح التشفير في اتجاه ما فإن المخترق ما زال بحاجة لمعرفة المفتاح الآخر لفك تشفير الرسالة في الاتجاه الآخر، لكن بالمقابل خوارزميات التشفير غير المتناظر أكثر تعقيداً حسابياً وتستهلك وقتاً أطولاً وطاقة حسابية أعلى من خوارزميات التشفير المتناظر.

– إنَّ آلية التشفير المستخدمة في شبكات الحساسات اللاسلكية الداعمة للوسائط المتعددة يجب أن تتماشى مع قيود العقد المكونة للشبكة وأن تكون مناسبة من حيث حجم البرامج اللازمة لتشغيلها، وحجم البيانات الناتج عن استخدامها، والوقت المستغرق في تنفيذها، و مستوى الطاقة التي تستهلكها [10].



الشكل (1) : مخطط التشفير غير المتناظر

2.1 خوارزمية تشفير المفتاح العام المعتمدة على أشباه الزّمر التربيعية متعددة المتحوّلات :

تُعدّ خوارزمية تشفير المفتاح العام المعتمدة على أشباه الزّمر التربيعية متعددة المتحوّلات Multivariate MQQ (quadratic quasigroups) أحد أصناف خوارزميات التشفير بالمفتاح العام المعتمدة على كثيرات الحدود التربيعية متعددة المتحوّلات MQPKC ، والتي تعتمد في مبدأ عملها على ثلاثة تحويلات أساسية سيتم شرحها لاحقاً، يعتمد التحويل المركزي في هذه الخوارزمية MQQ على بنى جبرية تُسمّى أشباه الزّمر. سنقدّم فيما يلي بعض المصطلحات الرياضيّة المتعلقة بهذه الخوارزمية [15,16,17].

1.2.1 أشباه الزّمر Quasigroups :

تعريف: شبه الزّمرة $(Q,*)$ هي بنية جبرية تتألف من مجموعة Q من العناصر مع عملية ثنائية $(*)$، بحيث تحقق القانون الآتي :

$$(\forall u, v \in Q)(\exists! x, y \in Q) \quad u * x = v \;\&\; y * u = v \qquad (1)$$

أي أنّه من أجل أي عنصرين $a, b \in Q$ يوجد عنصرين فريدين $x, y \in Q$ بحيث يكون:

$$a * x = b \quad , \quad y * a = b$$

$$x * y = z \Leftrightarrow y = x\backslash z \Leftrightarrow x = z/y \qquad (2)$$

حيث أنّ (/) و (\ ) هي عمليات ثنائية أيضاً، و نسمّي كل من $(Q,/)$ و $(Q,\backslash)$ شبه زمرة.

- من أجل استخدام أشباه الزّمر في خوارزميات MQPKC، نمثلها كتوابع بولينية vector (v.v.b.f) valued Boolean functions، ولهذا نختار تابعاً تقابلياً (bijection)

$\beta: Q \to \{0,1, \dots \dots, 2^d - 1\}$ ، حيث يتم تمثيل كل عنصر $a \in Q$ بسلسلة فريدة من البتات $(x_1, x_2, \dots \dots, x_d) \in \{0,1\}$.

لذاس يكون لدينا v.v.b.f من أجل شبه زمرة $(Q,*)$ معطاة :

$$* vv : \{0,1\}^{2d} \to \{0,1\}^d$$

$$a * b = c \Leftrightarrow * vv(x_1, x_2, \dots \dots, x_d, y_1, y_2, \dots \dots, y_d) = (z_1, z_2, \dots \dots, z_d) \qquad (3)$$

حيث أنّ $(x_1, x_2, \dots \dots, x_d)$ هو التمثيل الثنائي للعنصر a، و $(y_1, y_2, \dots \dots, y_d)$ هو التمثيل الثنائي للعنصر b، و$(z_1, z_2, \dots, z_d)$ هو التمثيل الثنائي للعنصر c و $z_i = f_i(x_1, x_2, \dots, x_d, y_1, y_2, \dots, y_d)$

ويمكن التعبير عن أي تابع بولياني $f = (x_1, x_2, \dots \dots x_k)$ بالشكل الجبري الطبيعي ANF (normal algebraic) form وفق القانون الآتي :

$$NF(f) = \propto_0 + \sum_{i=1}^{k} \propto_i x_i + \sum_{1 \le i < j \le k} \propto_{i,j} x_i x_j + \sum_{1 \le i < j < s \le k} \propto_{i,j,s} x_i x_j x_s + \cdots \qquad (4)$$

حيث أنّ $\propto_0, \propto_i, \propto_{i,j}, \dots \dots \in \{0,1\}$ وعمليات الجمع والضرب تتم في $GF(2)$.

إنّ الـ ANFs تعطينا معلومات عن درجة تعقيد شبه الزمرة وذلك من خلال درجة التوابع البوليانية f_i ، حيث أنّه كلّما ارتفع العامل d لشبه الزّمرة، سوف يرتفع معه درجة كثيرات الحدود $ANF(f_i)$.

2.2.1 تحويلات سلاسل أشباه الزّمر quasigroups string transformation:

بفرض لدينا شبه الزمرة $(Q,*)$ تحوي n عنصر، وبفرض لدينا السلسلة $M = a_1 a_2 \dots \dots a_n$

حيث أنّ $a_i \in Q$ ، و بفرض لدينا العنصر القائد (leader) هو $l \in Q$ ، فإنّ هناك تحويلين أساسيين هما e-transformation و d- transformation:

$$e_{l,*}(M) = b_1 b_2 \dots . b_n \Leftrightarrow \ b_1 = l * a_1 \ , b_2 = b_1 * a_2, \dots \dots, \ b_n = b_{n-1} * a_n \quad (5)$$

$$d_{l,*}(M) = c_1 c_2 \dots . c_n \Leftrightarrow c_1 = l * a_1 \ , c_2 = a_1 * a_2, \dots \dots, c_n = a_{n-1} * a_n \quad (6)$$

3.2.1 أشباه الزّمر التربيعية متعددة المتحوّلات :

عموماً عند توليد أشباه زمر بشكل عشوائي بعامل 2^d حيث $d \leq 4$ ، فإنّ درجة كثيرات الحدود ستكون أعلى من2، ومثل أشباه الزّمر هذه غير مناسبة لاستخدامها في خوارزميات MQPKC، لذلك لا بدّ من تحديد الشروط اللازمة لتكون أشباه الزّمر من النوع MQQ .

تعريف : نقول عن شبه زمرة $(Q, *)$ بعامل 2^d بأنّها شبه زمرة تربيعية متعددة المتحوّلات (MQQ) من النمط $quad_{d-k} lin_k$ إذا كان هناك $d - k$ كثير حدود من الدرجة الثانية (تربيعية)، وكان هناك k كثير حدود من الدرجة الأولى(خطّية) وذلك عند تمثيلها بالشكل ANF، حيث $0 \leq k < d$ [21].

يمكن وصف عملية توليد أشباه الزمرة التربيعية متعددة المتحولات MQQs وفق المعادلة الآتية [18,21]:

$$X * Y \equiv B.U(X).A_2.Y + B.A_1.X + C \quad (7)$$

حيث أنّ: $X = (x_1, \dots \dots, x_d)$ و $Y = (y_1, \dots \dots, y_d)$

و المصفوفات A_1 , A_2 , B هي مصفوفات قابلة للعكس وكل منها بحجم $d \times d$ وتولد عناصرها بشكل عشوائي في$GF(2)$. و الشعاع C بطول d تولد عناصره عشوائيّاً في $GF(2)$.

المصفوفة $U(X)$ هي مصفوفة مثلثية عليا وعناصر القطر الرئيسي تساوي الواحد، والعناصر فوق القطر الرئيسي هي عناصر خطية وتابعة للمتغيرات $X = (x_1, \dots \dots, x_d)$، ويمكن حسابها وفق المعادلة الآتية:

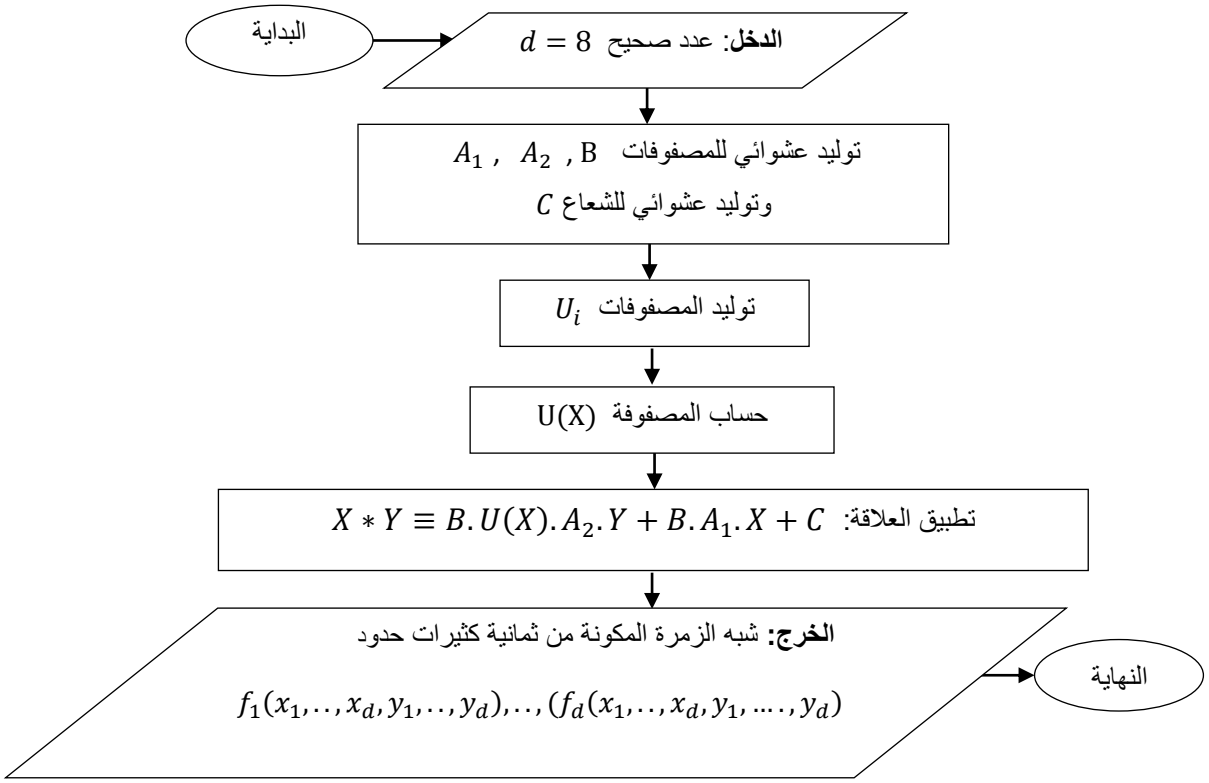
$$U(X) = I + \sum_{i=1}^{d-1} U_i . A_1 . x \quad (8)$$

تكون كل عناصر المصفوفات U_i صفرية ما عدا العناصر التي تقع في الأسطر $\{1, .., i\}$ فتكون إما 0 أو 1.

عندئذٍ سنحصل على أشباه الزّمر

$$* vv(x_1, \dots, x_d, y_1, \dots, y_d) = \left(f_1(x_1, \dots, x_d, y_1, \dots, y_d), \dots, f_d(x_1, \dots, x_d, y_1, \dots, y_d)\right) (9)$$

ويبين المخطط الآتي خطوات توليد شبه الزمرة MQQ من أجل العامل $d = 8$:



الشكل (2) : مخطط توليد شبه الزمرة بعامل $\mathbf{d = 8}$ [18]

2. خوارزمية التشفير MQQ-ENC :

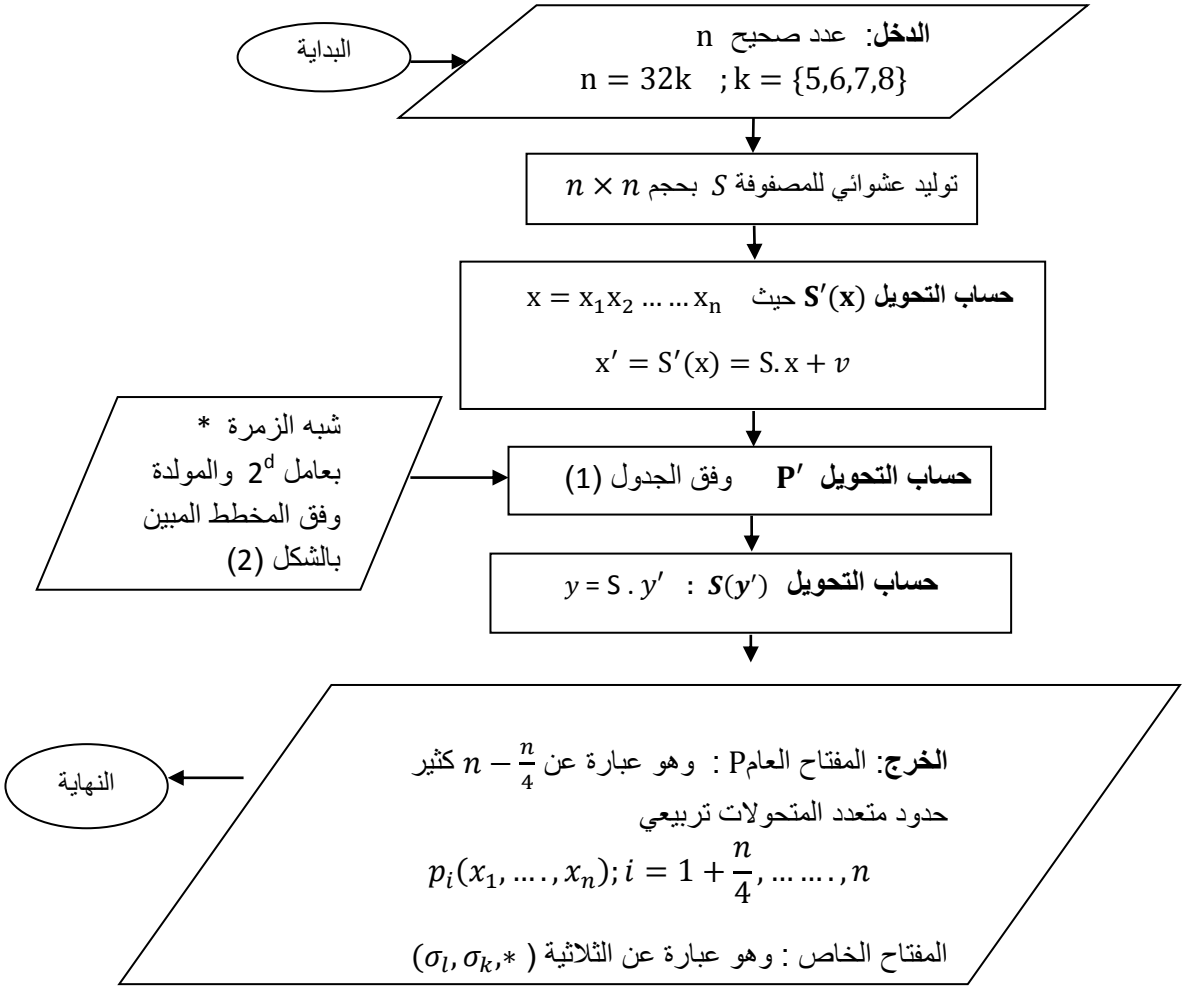
يُعطى الشكل العام لمخطط خوارزمية MQQ بالشكل الآتي: $S^\circ P'^\circ S' : \{0,1\}^n \rightarrow : \{0,1\}^n$

- حيث : $S' = S.x + v$ هو عبارة عن تحويل خطّي تقريبي(affine) أما التحويل S هو تحويل خطي (linear) ، و التحويل P' هو التحويل التربيعي المركزي (multivariate quadratic) [18] .
- الشعاع v بولياني طوله n بت. ويبين الجدول الآتي وصفاً للتحويل المركزي P':

الجدول (1): خطوات التحويل المركزي $P'(X)$

الدخل: الشعاع $x' = (f_1, \dots.., f_n)$ والذي يتألف من n تابع خطّي وكل منها تابع لـ n متحوّل $n = 32k \quad ; k = 5,6,7,8$
الخرج: y' ومؤلف من 8 توابع خطية $P_i'(x_1, \dots., x_n) , i = 1, \dots.,8$ و $n-8$ كثير حدود تربيعي متعدد المتحولات $P_i'(x_1, \dots., x_n), i = 9, \dots., n$
الخطوات: 1. تمثيل الشعاع $x' = f_1..f_n$ كسلسلة $x' = X_1X_2 \dots X_{n/8}$ ، حيث X_i أشعة كل منها 8 بت 2. حساب $y' = Y_1Y_2 \dots \dots Y_{n/8}$ حيث : $Y_1 = X_1$ $Y_{j+1} = X_j * X_{j+1}$ من أجل الأعداد الزوجية $j = 2,4,..$ $Y_{j+1} = X_{j+1} * X_j$ من أجل الأعداد الفردية $j = 3,5,...$

يبين المخطط الآتي آلية توليد زوج المفاتيح (عام & خاص) وفق خوارزمية MQQ [18]:



الشكل (3) : مخطط توليد زوج المفاتيح (عام & خاص) وفق خوارزمية MQQ

1.2. مخطط التشفير MQQ-ENC:

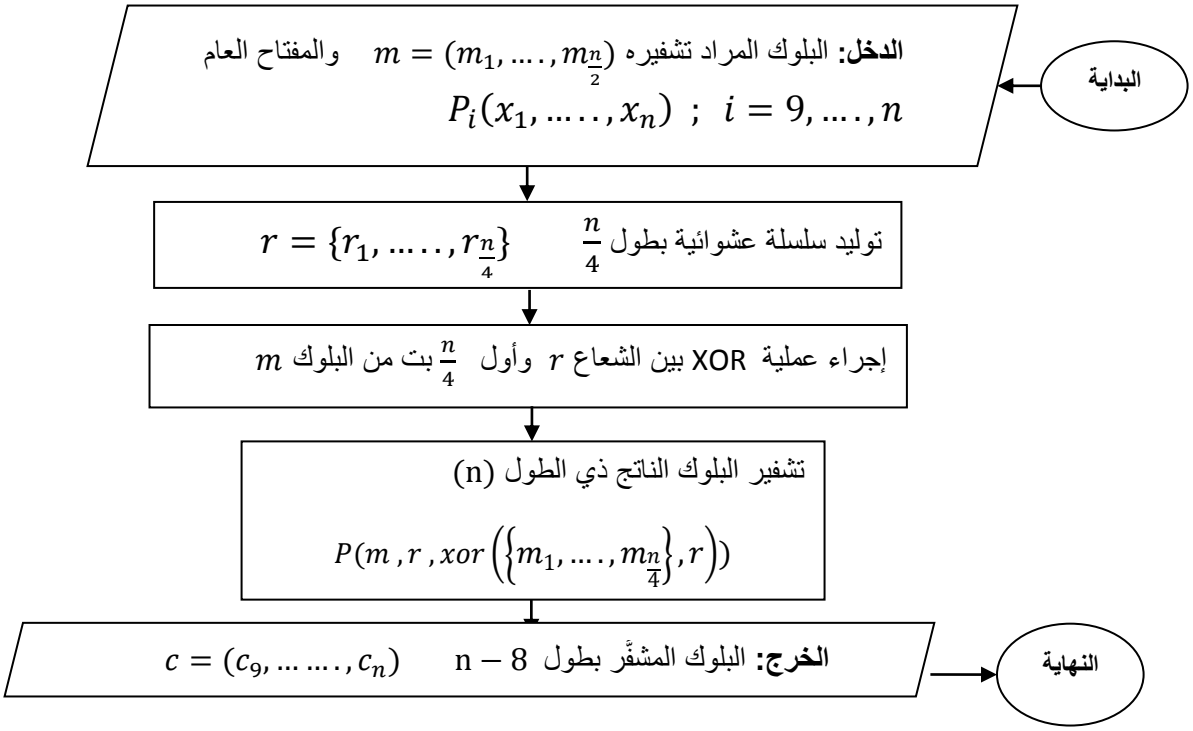
يُعطى الشكل العام لعملية التشفير وفق خوارزمية MQQ بواسطة المفتاح العام وفق المعادلة الآتية:

$$y(y_1, \dots., y_n) = P_i(x_1, \dots., x_n) \; ; \; i = 1, \dots., n \qquad (10)$$

بداية يقسم الملف المراد تشفيره وذي الطول غير المحدّد إلى بلوكات كل منها بطول (n)، ويشفر كل بلوك على حدا، ومن ثمّ تجمع هذه البلوكات للحصول على الملف المُشَفَّر.

ولكن: عند توليد زوج المفاتيح (عام & خاص) وفق الخوارزمية الموضّحة في الشكل (3) سنحصل على المفتاح العام P بطول $n - \frac{n}{4}$ $P_i(x_1, \dots., x_n) \; ; \; i = 1 + \frac{n}{4}, \dots., n$ وهذا الطول غير متوافق مع طول البلوك المراد تشفيره وهو (n). لأنّه وفقاً لهذه العملية سيتم تشفير بلوك بطول n والحصول على بلوك مشفَّر بطول $n - \frac{n}{4}$ وبالتالي لن نتمكن من فك تشفير هذا البلوك في جهة المستقبِل. **فكانت فكرة الحل كالآتي:**

1. تغيير حجم المفتاح العام: أجرينا تعديلاً على خوارزمية توليد المفاتيح المبينة سابقاً بحيث نحصل على مفتاح عام P بطول $n-8$ $P_i(x_1,\dots\dots,x_n)\ ;\ i=9,\dots,n$
2. مرحلة التهيئة: تقسيم الملف (M) المراد تشفيره وذي الطول غير المحدد إلى بلوكات كل منها بطول $\frac{n}{2}$ وتشفير كل جزء على حدا، ثمّ تجميع البلوكات المشفَّرة للحصول على الملف المشفَّر (M')
3. من أجل كل بلوك بطول $\frac{n}{2}$ ستنفذ عملية التشفير وفق خوارزمية MQQ – ENC كما هو موضح في المخطط الآتي[18]:



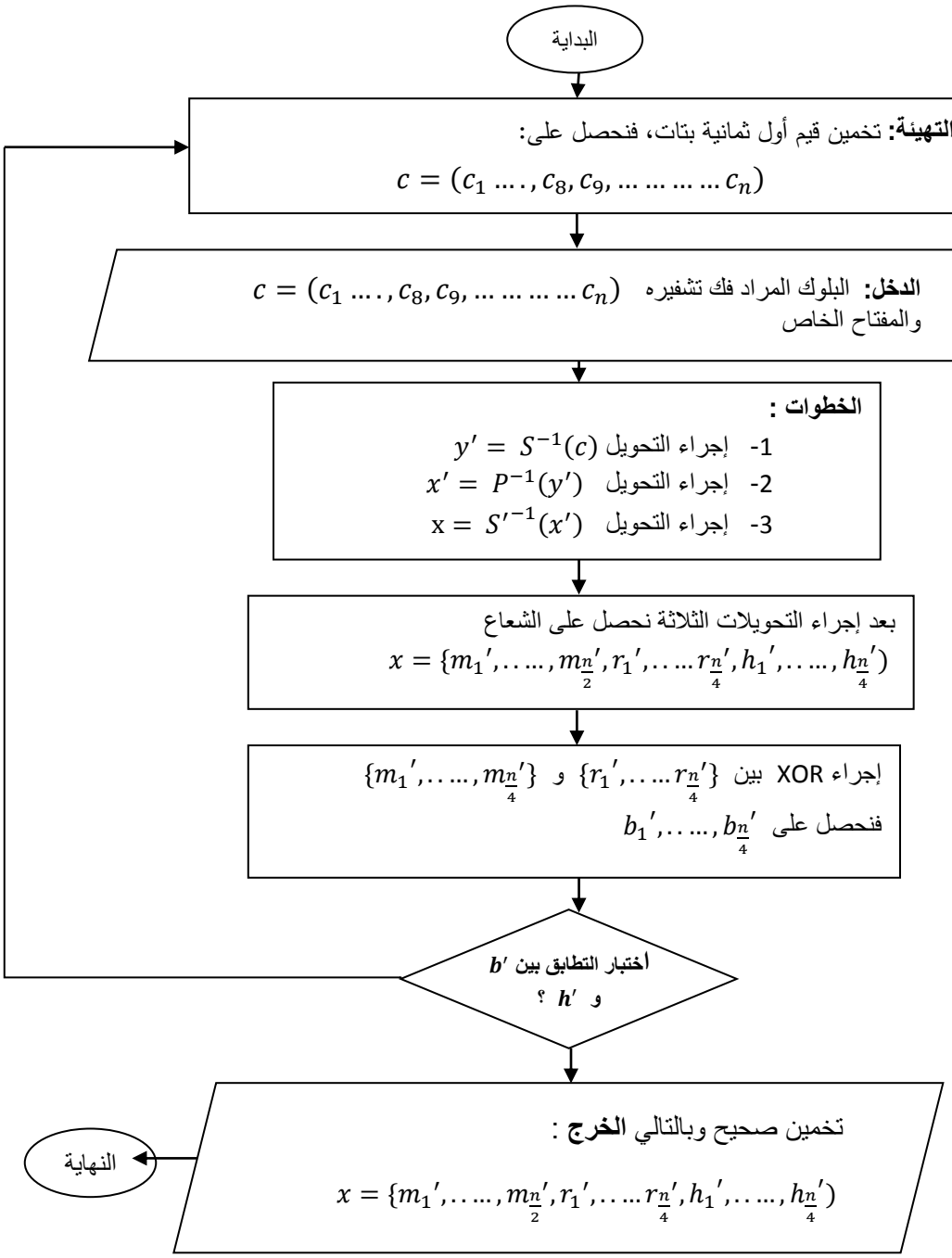
الشكل (4) : مخطط عملية التشفير وفق خوارزمية MQQ

وبذلك بهذه الطريقة يشفر كل بلوك بطول $\frac{n}{2}$ بسلسلة طولها n − 8.

<u>عملية فك التشفير</u>: يفك تشفير كل بلوك $c=(c_9,\dots\dots\dots,c_n)$ على حدا، كل بلوك بطول n − 8، ولكن يجب أن يكون طول البلوك المراد فك تشفيره يساوي n ، لذلك سنخمن قيم أول ثمانية بتات، فنحصل على:

$$c=(c_1\dots\dots,c_8,c_9,\dots\dots\dots\dots c_n)$$

ومن ثمّ ستنفذ عملية فك التشفير لهذا البلوك وفق المخطط الآتي [18] :



الشكل (5) : مخطط عملية فك التشفير وفق خوارزمية MQQ

3. خوارزمية RSA :

تعد خوارزمية RSA أوّل خوارزمية تشفير غير متناظر والتي نشرت في عام 1978، و ما تزال مستخدمة حتى الآن في العديد من التطبيقات مثل البطاقات البنكية. تعتمد هذه الخوارزمية في أمنها على صعوبة تحليل أعداد أوّلية كبيرة جدّاً إلى عواملها الأولية [10]. يولد زوج المفاتيح (عام &خاص) وفق خوارزمية RSA من خلال الخطوات الآتية:

1- اختيار عددين أوّليين كبيرين $\boldsymbol{p, q}$، حيث $\boldsymbol{p \neq q}$.

2- حساب $\boldsymbol{n = p \times q}$

3- حساب معامل أولر $\boldsymbol{\varphi(n) = (p-1)(q-1)}$

4- اختيار العامل e بحيث تحقق العلاقة الآتية: $1 < e < \varphi(n)$

حيث e و $\varphi(n)$ عددين أوليين فيما بينهما

5- حساب العامل d حيث : $e * d = 1(mod\ \varphi(n))$

نحصل بذلك على زوج المفاتيح : المفتاح العام : (e, n) ، المفتاح الخاص : (d, n)

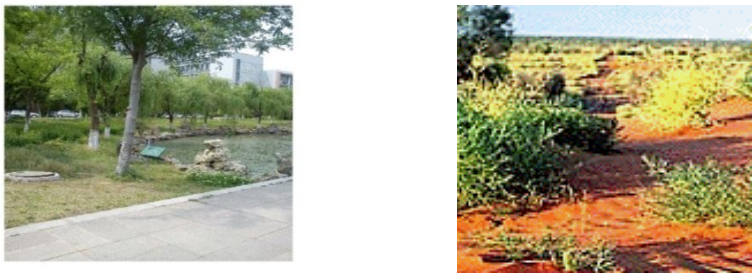
عملية التشفير: تتم باستخدام المفتاح العام وفق العلاقة الآتية: $c = m^e\ mod\ n$

عملية فك التشفير: تتم باستخدام المفتاح الخاص وفق المعادلة الآتية: $m = c^d\ mod\ n$

حيث m هي الرسالة المراد تشفيرها، و c هي الرسالة المُشفّرة.

النتائج والمناقشة:

اخترنا نموذجين من الصور الملوّنة بأحجام مختلفة، وهذه الصور ملتقطة بواسطة كاميرا حساس لاسلكي مخصّص لمراقبة البيئة. وهي مبينة في الشكل الآتي: الصورة الأولى بحجم 29.3KByte وامتدادها png، والصورة الثانية بحجم 268KByte وامتدادها jpg.



الشكل (6) : نموذجا الصور المستخدمة في عملية المحاكاة

تُعدّ هذه الصور من أشهر صور الحساسات اللاسلكية المستخدمة كنماذج اختبارية في الأبحاث العلمية [19]. طبقت خوارزمية المفتاح العام MQQ-ENC المدروسة آنفاً على نموذجي الصور المختارة، واختبرت هذه الخوارزمية وقورنت مع خوارزمية المفتاح العام الشهيرة RSA عند تطبيقها على نفس الصور.

ونفذت الخطوات السابقة على جهاز حاسب ذو المواصفات المبينة في الجدول الآتي :

الجدول (2) : بعض مواصفات الجهاز الذي طبقت عليه المحاكاة

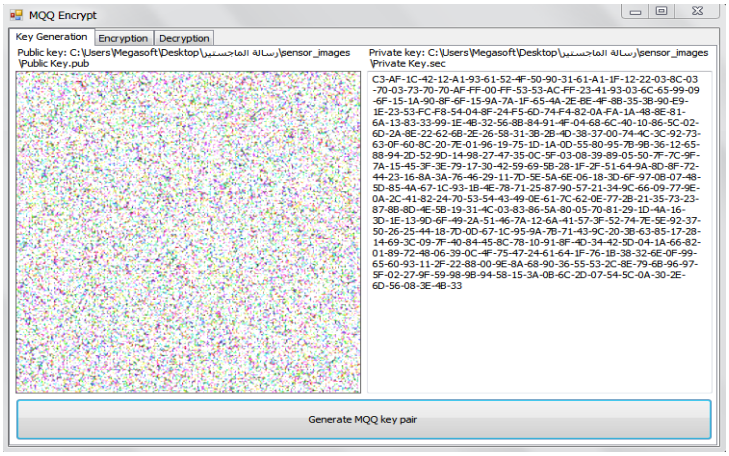
نظام التشغيل Operating system	المعالج Processor	نوع النظام System type	ذاكرة الوصول العشوائي RAM
Windows 7 Ultimate	Intel(R)Core(TM)i5-2410M CPU @2.30GHz	64-bit	4GB

اعتمدنا في عملية التحليل والمقارنة على مجموعة من البارامترات الهامة لتقييم الأداء وهي: أحجام المفاتيح المولّدة والصور المشفرة، وسرعة التنفيذ، والحيز المحجوز من ذاكرة الحساس اللاسلكي، ودرجة تعقيد الخوارزمية.

1. سيناريو العمل:

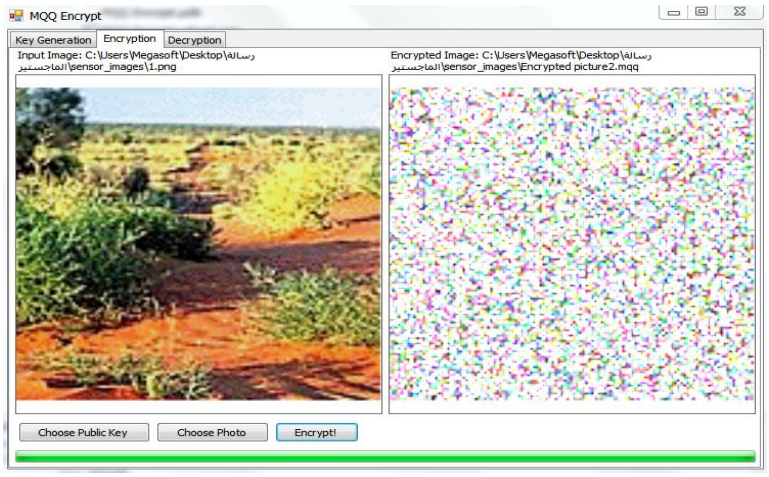
السيناريو الأول: قمنا في هذا السيناريو بتطبيق خوارزمية المفتاح العام MQQ بمراحلها الثلاثة (توليد المفاتيح، التشفير، فك التشفير) على نموذجي الصور المدروسة وذلك من أجل n=160 .

أوّلاً: ولدت زوج المفاتيح وفق الخوارزمية المشروحة في الفقرة (1.2) وحصلنا على زوج المفاتيح الموضح في الشكل الآتي، تمّ عرض المفتاح العام بشكل صورة بسبب كبر حجمه، أما المفتاح الخاص فتم عرضه بشكل ست عشري.



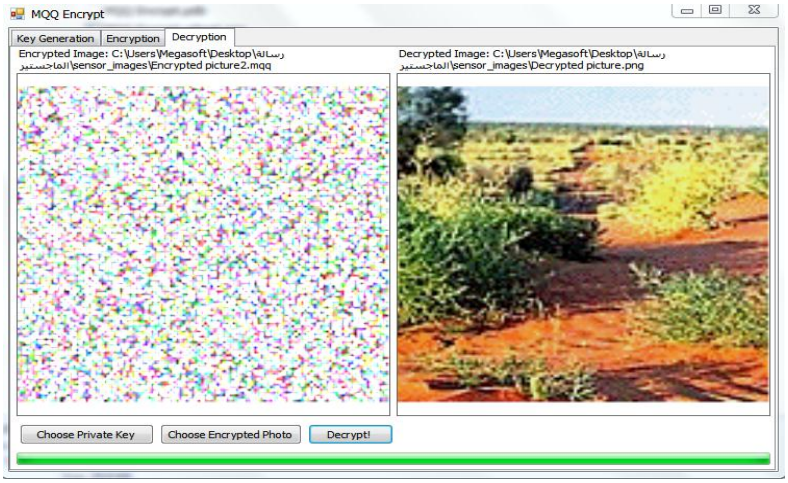
الشكل (7) : زوج المفاتيح (عام & خاص) المولد وفق خوارزمية MQQ-ENC

ثانياً: شفرت الصور المدروسة باستخدام المفتاح العام وفق الخوارزمية المبينة في الشكل (4)، ويبين الشكل الآتي إحدى الصور المدروسة قبل التشفير والصورة الناتجة بعد التشفير.



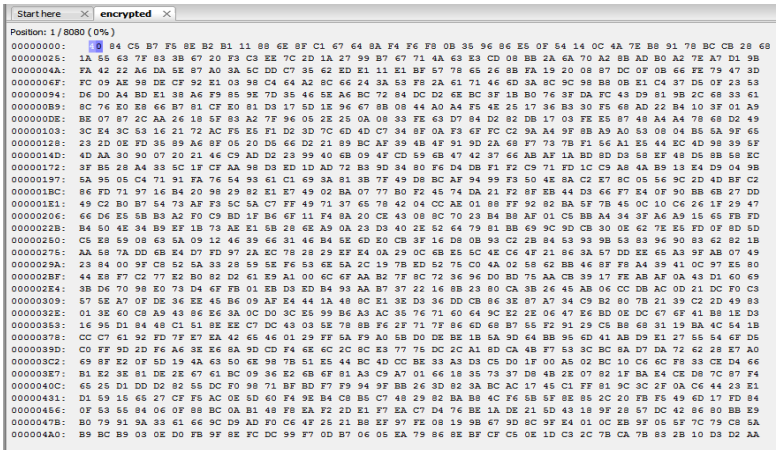
الشكل (8) : نتيجة تشفير إحدى الصور المدروسة

ثالثاً: فك تشفير الصور المدروسة – والتي شفرت في الخطوة السابقة– باستخدام المفتاح الخاص وفق الخوارزمية المبينة في الشكل (5)، يبين الشكل الآتي نتيجة فك التشفير لإحدى الصور المشفّرة:



الشكل (9) : نتيجة فك تشفير إحدى الصور المشفرة

السيناريو الثاني: تمّ تشفير وفك تشفير الصور المدروسة باستخدام خوارزمية RSA-1024، ويبين الشكل الآتي إحدى الصور المدروسة المشفرة وفق خوارزمية RSA-1024 :



الشكل (10) : الصورة الأولى المشفّرة وفق RSA

2. التحليلات والمناقشة:

سنورد فيما يأتي مناقشة النتائج التي حصلنا عليها وتحليل بعض البارامترات الخاصة بالخوارزمية.

1- مستوى الأمن المحقق :

ذكرنا سابقاً أنّ خوارزمية RSA تعتمد في تحقيق أمنها على صعوبة تحليل أعداد أوّلية كبيرة إلى عواملها الأوّلية، وبالنتيجة من أجل $n = 1024$ bit يزداد التعقيد الحسابي للخوارزمية والناتج عن كون العددين الأوليين p , q يجب أن يكونا كبيرين لأنّ $\boldsymbol{n = p \times q}$ ، إضافة إلى التعقيد الحسابي الناتج عن استخدام تابع modular لحساب $mod\ \varphi(n)$. إنّ هذا التعقيد الحسابي لدى تطبيق خوارزمية RSA-1024 يحقق نفس مستوى الأمن الذي تحققه خوارزمية MQQ-160 والتي

تعتمد في عملها على عمليات AND و XOR المنطقية والتي تُعدّ أقل تعقيداً حسابياً وأكثر بساطة وأسرع في التنفيذ من التوابع المستخدمة في خوارزمية RSA.

2- أحجام المفاتيح و الصور المشفرة:

يتكوّن المفتاح العام الناتج وفق خوارزمية MQQ من n معادلة تربيعية متعددة المتحولات، وكل معادلة تتألف من جزء ثابت، و n جزء خطّي، و $\frac{n\times n-n}{2}$ جزء تربيعي، ترتبط هذه الأجزاء مع بعضها وفق عمليات منطقية هي (XOR و AND) والتي تمثّل عمليات الجمع والضرب في المعادلة.

- يُعطى حجم المفتاح العام بالعلاقة الآتية [15] :

$$n \times \frac{1+\frac{n(n+1)}{2}}{8\times 1024} \quad KByte \qquad (11)$$

بالنسبة لخوارزمية MQQ-ENC التي درسناها سابقاً فإنّ المفتاح العام يتكون من $n-8$ معادلة تربيعية متعددة المتحولات، لذا يُعطى حجم المفتاح العام بالعلاقة الآتية:

$$(n-8) \times n \times \frac{1+\frac{n(n+1)}{2}}{8\times 1024} \quad KByte \qquad (12)$$

أما المفتاح الخاص وفق خوارزمية MQQ فيتألف من شبه الزّمرة التربيعية المولّدة بعامل 2^8 ممثلة بـ $81\ byte$ ، إضافة للمصفوفة S البوليانية والتي تمّ تمثيلها بطريقة معينة ليكون حجمها 2n Byte ، فيُعطى حجم المفتاح الخاص حسب العلاقة الآتية:

$$2n+81 \quad Byte \qquad (13)$$

يبيّن الجدول الآتي أحجام المفاتيح والصور المشفرة التي حصلنا عليها لدى تطبيق خوارزمية MQQ من أجل $n = 160$ و خوارزمية RSA من أجل $n = 1024$.

الجدول (3) : أحجام المفاتيح الناتجة وأحجام الصور بعد التشفير

الخوارزمية	المفتاح العام	المفتاح الخاص	الصورة المدروسة	
			الصورة الأولى (29.3 KB)	الصورة الثانية (268 KB)
MQQ-160	244.758 KB	401 Byte	55.7 KB	509 KB
RSA-1024	278 Byte	902 Byte	32.1 KB	293 KB

يتبين لنا من الجدول السابق أن حجم المفتاح المستخدَم في عملية التشفير قد ارتفع حجمه عن حجم المفتاح العام المعطى بالعلاقة (11). وهذا ناتج عن كوننا عدّلنا في خوارزمية توليد المفتاح العام، إذ أصبح يتكون من $n-8$ معادلة تربيعية متعددة المتحولات بدلاً من n ، وذلك من أجل إتمام عمليتي التشفير وفك التشفير بنجاح. ولكن هذا التعديل أدّى أيضاً إلى زيادة حجم الصورة بعد تشفيرها بالمفتاح العام إلى ضعف حجمها الأصلي تقريباً إذ أنّه تمّ تشفير كل $(\frac{n}{2})$ بت فعلية بـ $(n-8)$ بت، بينما في خوارزمية RSA-1024 فإنّ حجم الصورة بعد التشفير يزداد بمقدار 10% فقط عن حجمها الأصلي.

في حال أن المفتاح العام يتألف من n معادلة تربيعية فلن يكون هناك زيادة في حجم الصورة عند تشفيرها بهذا المفتاح العام، لأنّه في هذه الحالة ستشفر كل (n) بت فعلية بـ (n) بت، ولكن بالمقابل سنحصل على مفتاح تشفير بحجم أكبر. إنّ

تخفيض حجم المفتاح العام بهذه الطريقة بمقدار K معادلة تربيعية، فإنّه في جهة الاستقبال بدايةً ستخمن الـ 2^K قيمة من أجل كل جزء مشفَّر بطول $(n-K)$، أي كلّما ازدادت قيمة K سيزداد عدد القيم التي ستخمن عند فك التشفير وهذا سيستهلك زمناً إضافياً. إنّ الحجم الكبير للمفتاح العام سيتطلّب حيز تخزين كبير من ذاكرة الحساس. إنّ الحجم الكبير للصورة المشفّرة سيؤثّر على عرض الحزمة المتوفّر وعلى الاستطاعة المستهلكة للعقدة عند الإرسال. لذا يجب أخذ هذه الأمور بالحسبان والمقايضة فيما بينها عند تطبيق خوارزمية MQQ في شبكات الـ WMSNs.

3- الزمن اللازم للتنفيذ (سرعة عملية التنفيذ مقدرة بالثانية):

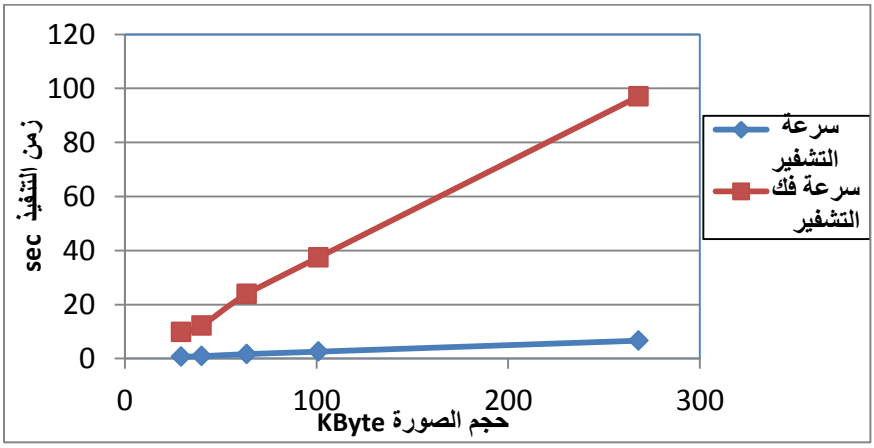
طبقنا أيضاً كل من خوارزميتي المفتاح العام MQQ-160 و RSA-1024 بمراحلهما الثلاثة (توليد المفاتيح، التشفير، فك التشفير) على نموذجي الصور المقترحة، وحصلنا على النتائج في الجدول الآتي:

الجدول(4) : سرعة عملية التنفيذ مقدرة بالثانية من أجل التشفير / فك التشفير

الخوارزمية	توليد المفاتيح	الصورة الأولى بحجم 29.3 KB		الصورة الثانية بحجم 268 KB	
		التشفير	فك التشفير	التشفير	فك التشفير
MQQ-160	0.634	0.751	9.85	6.644	97.83
RSA-1024	0.25	24.13	24.92	225.40	228.32

يتبين لنا من هذا الجدول عدّة نقاط:

- تتفوق خوارزمية MQQ على خوارزمية RSA من حيث سرعة عمليتي التشفير وفك التشفير، إذ أنّ MQQ-160 أسرع في إنجاز عملية التشفير بحوالي 30 مرّة، وأسرع في إنجاز عملية فك التشفير بحوالي 3 مرّات من خوارزمية RSA-1024.
- في خوارزمية RSA إنّ سرعة عملية التشفير تقارب سرعة عملية فك التشفير وذلك من أجل صورة معينة مدروسة، أمّا في خوارزمية MQQ نلاحظ أنّ سرعتها في إنجاز التشفير أكبر من سرعتها في إنجاز فك التشفير بشكل واضح.
- إنّ حجم الصورة المدروسة يؤثّر بشكل واضح على سرعة كل من عمليتي التشفير وفك التشفير. من أجل خوارزمية MQQ-160 – المبينة في الشكلين (4) و (5)– عمَّمنا الدراسة لتشمل عدّة صور ملتقطة بواسطة كاميرا حسّاس لاسلكي، وبأحجام مختلفة، فحصلنا على المخطط البياني الموضح في الشكل (11):



الشكل (11) : مخطط بياني يبين العلاقة بين حجم الصورة وسرعة تشفيرها وفك تشفيرها

نلاحظ من المخطط البياني السابق أن زمن تشفير الصورة يزداد بازدياد حجم الصورة، ولكن هذه الزيادة ليست واضحة كما هو في حالة فك التشفير، إذ أنّ ازدياد حجم الصورة يؤدي إلى زيادة زمن عملية فك التشفير بشكل واضح.

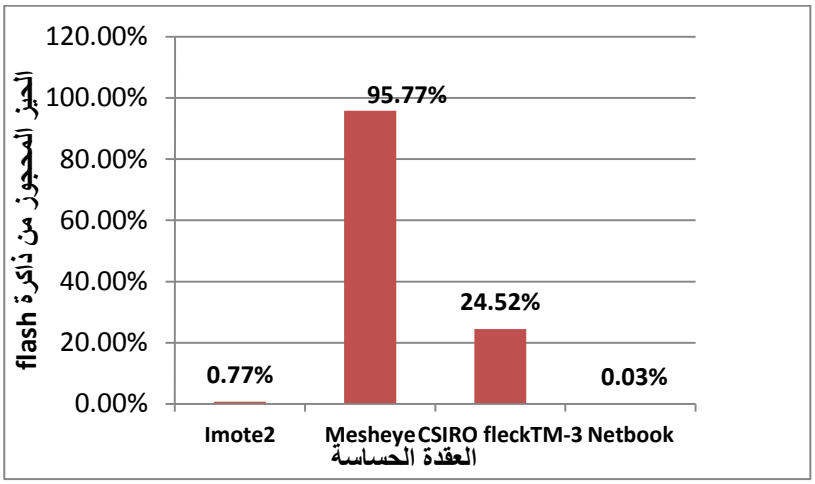
4- الحيز المحجوز من ذاكرة الحساس اللاسلكي:

اخترنا عدّة نماذج من الحساسات اللاسلكية الداعمة للوسائط المتعددة والمتوفرة في الأسواق لدراسة مدى ملائمة تطبيق خوارزمية المفتاح العام MQQ في هذه الحساسات.

بما أن زوج المفاتيح (عام & خاص) يخزن ضمن ذاكرة الـ flash لعقدة الحساس، فيكون الحجم اللازم لتحزين زوج المفاتيح هو حجم المفتاح العام مضافاً إليه حجم المفتاح الخاص، وبالنتيجة فإن حجم زوج المفاتيح يساوي:

244758+401=245159 Bytes

يبين المخطط البياني الآتي النسبة المئوية للحيز المحجوز من ذاكرة flash للعقدة واللازم لتخزين زوج المفاتيح المولّدة وفق خوارزمية MQQ -160.



الشكل (12) : مخطط بياني يبين النسبة المئوية للحيز المحجوز من حجم ذاكرة flash للعقدة الحساس

نلاحظ من المخطط البياني أنّ الحجم اللازم لتخزين المفاتيح يكون أصغريّاً في كل من النموذجين Imote2 و Netbook، بينما يظهر تأثير الحجم الكبير للمفتاح العام بالنسبة للنموذج CSIRO fleckTM-3 وتقريباً ربع ذاكرة الـ flash بالنسبة لخوارزمية MQQ-ENC، أمّا بالنسبة للنموذج Mesheye فإنّ حجم ذاكرة الـ flash لا يعُدّ مناسباً لتخزين مفاتيح بهذه الأحجام، وهذا ما يجب أخذه بالحسبان عند تطبيق خوارزمية المفتاح العام MQQ ضمن شبكة WMSNs، إذ يجب اختيار النوع المناسب من العقد الحساسة.

5- درجة تعقيد الخوارزمية :

من خلال المقارنة بين درجتي التعقيد لكل من خوارزميتي المفتاح العام MQQ و RSA، نلاحظ أن عملية التشفير في كل منهما تمتلك درجة تعقيد من النوع التكعيبي (cubic) أيّ $O(N^3)$، حيث أنّ N يمثّل حجم الدخل، بغضّ النظر عن أنّ خوارزمية الضرب والتربيع تأخذ بالحسبان اللوغاريتم الثنائي لحجم الدخل في خوارزمية RSA . أمّا بالنسبة لعملية فك التشفير فإنّ خوارزمية MQQ تمتلك درجة تعقيد من النوع التربيعي (quadratic) أي $O(N^2)$، أمّا عملية فك التشفير في RSA فهي أعقد من MQQ إذ أنها من النوع التكعيبي. وحسب ترتيب توابع درجة التعقيد يتبين لنا أنّ توابع درجة التعقيد من النوعين التكعيبي والتربيعي هي من النوع سهل الحل نسبياً، فهي ليست من النوع المعقد وصعب الحل جدّاً والذي يتطلب

قدرات معالجة إضافية ومنه استهلاك أكثر لاستطاعة العقدة الحساسة، كما أنّها ليست من النوع السهل جدّاً والذي يمكن إنجازه ببساطة ومنه عدم إمكانية كسر الخوارزمية بسهولة.

الاستنتاجات والتوصيات:

درسنا في هذا البحث خوارزمية المفتاح العام MQQ، وتطبيق التشفير MQQ-ENC من أجل n=160 على صور ملتقطة بواسطة عقدة حساس لاسلكي، وذلك لدراسة مدى فعالية تطبيق هذه الخوارزمية في شبكات الحساسات اللاسلكية الداعمة للوسائط المتعددة.

من خلال الدراسة و مناقشة النتائج تبين لنا أنّ خوارزمية المفتاح العام MQQ المعتمدة على أشباه الزّمر التربيعية متعددة المتحوّلات قد حققت أداء جيّداً مقارنةً مع خوارزمية RSA، فمن خلال الدراسة النظرية للخوارزمية لاحظنا أنها تعتمد في أمنها على صعوبة حل عدد كبير من المعادلات غير الخطية، لأنّ ذلك سيتطلّب وقتاً وجهداً كبيرين وبالتالي صعوبة كسر هذه الخوارزمية. ومن خلال التطبيق العملي تبين لنا ما يأتي:

1- أظهرت خوارزمية MQQ سرعة عالية في تنفيذ عمليات التشفير وفك التشفير تفوق سرعة خوارزمية المفتاح العام الشهيرة RSA، وهذا ناتج عن كونها تعتمد في أساس عملها على عمليات XOR و AND وهي عمليات منطقية بسيطة لا تتطلّب معالجة حسابية عالية و تُنجَز بسرعة كبيرة، فهي بذلك تناسب شبكات الحساسات اللاسلكية الداعمة للوسائط المتعددة التي تتطلب في العديد من التطبيقات سرعة عالية في التنفيذ والإرسال في الزمن الحقيقي. ولاحظنا تأثير حجم الصور على سرعة عمليتي التشفير وفك التشفير.

2- يُعدّ الحجم الكبير للمفتاح العام قضيّة مهمّة يجب أخذها بالحسبان، فكما لاحظنا من النتائج التي توصّلنا إليها أنّ حجم المفتاح العام في خوارزمية MQQ أكبر بحوالي 10^3 مرّة من المفتاح العام لخوارزمية RSA . وهذا يُعدّ نقطة حرجة عند تطبيق خوارزمية MQQ في شبكات الـ WMSNs كون العقد ذات سعات تخزينية محدودة. لذلك يجب أخذ نوع العقد الحسّاسة المستخدمة والسعات التخزينية المتاحة فيها بالحسبان، وبالتالي مدى إمكانية ملاءمتها لتطبيق خوارزمية المفتاح العام MQQ .

3- إنّ خوارزمية MQQ لا تسبب زيادة على حجم الصورة بعد تشفيرها، وهذا يُعدّ ميّزة جيّدة لهذه الخوارزمية، لأنّ الزيادة على حجم الصور المشفرة الناتج عن تقنيات التشفير يُعدّ أمراً غير مرغوب فيه، باعتبار أنّ ذلك سيتطلّب عرض حزمة إضافي واستهلاكاً أكبر لطاقة الإرسال للعقدة الحساسة. ولكن تخفيض حجم المفتاح العام في خوارزمية MQQ أدّى إلى زيادة حجم الصورة المشفّرة بشكل كبير، وهذا ما يجب مراعاته عند العمل على إيجاد إجرائيات لتخفيض حجم المفتاح العام.

4- اعتماداً على المبدأ العام الذي يقول أنّ الخوارزمية ذات زمن التنفيذ الأقل، ودرجة التعقيد O الأخفض هو دليل على أنّها ذات استهلاك الاستطاعة الأقل[20]، فإنّ ذلك يعطي مؤشّراً على أنّ خوارزمية المفتاح العام MQQ تتطلب استهلاك استطاعة أقل من خوارزمية المفتاح العام RSA.

5- إنّ خوارزمية MQQ المدروسة في هذا البحث طبقت من أجل n=160، واعتمدت على أشباه الزّمر التربيعية متعددة المتحوّلات بعامل d=8، وقد حققت بالرّغم من حداثتها أداءً جيّداً مقارنة مع أشهر خوارزميات المفتاح العام وأكثرها تطبيقاً، لذا نقترح في نهاية بحثنا هذا بإجراء دراسات معمّقة أكثر حول هذه الخوارزمية، ودراسة بارامتراتها الرياضيّة، وإجراء أبحاث حول إمكانية تخفيض حجم المفتاح العام، دون أن يؤثّر بشكل كبير على سرعة الخوارزمية وأمنها. كما نقترح تطبيق

الخوارزمية من أجل قيم أكبر لـ n (192, 224, 256)، ومن أجل أشباه زمر بعامل (d >8)، ودراسة تأثير ذلك على أداء الخوارزمية. بالإضافة إلى دراسة طرائق أخرى لتوليد أشباه الزّمر بسرعة وكفاءة عالية.

References:

[1] SINGH, R. and PANT, M., *Wireless Multimedia Sensor Networks: A review*. IJETST, Vol.01, 2014, pp. 134 -136.

[2] DANG, K.; SUN, H.; CHANET, P.; GARCIA-VIDAL, J.; BARCELO-ORDINAS, M.; SHI, M. and HOU, L., *Wireless Multimedia Sensor Network for plant disease detections.* New Information Communication Science and Technology for Sustainable Development International Workshop, 2013, pp.1 - 6.

[3] PRABHU, N.; RANJEETH KUMAR, C. and MOHANKUMAR B., *Energy-efficient and Secured Data Gathering in Wireless Multimedia Sensor Networks*. International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 2, 2014, pp. 3073-3079.

[4] ZAPATA, M.; ZILAN, R.; BICAKCI, K.; TAVLI, B. and BARCELÓ-ORDINAS, J., *The future of security in Wireless Multimedia Sensor Networks.* Springer Science +Business Media, LLC, Vol. 45, No. 1, 2009, pp.77-91.

[5] HUANG, Y., LIU, F. and YANG, B., *Public-Key Cryptography from New Multivariate Quadratic Assumptions* . International Association for Cryptologic Research, 2012, pp. 190 –205.

[6] http://bench.cr.yp.to/supercop.html. Last visit at 1/11/2020.

[7] www.microsoft.com . Last visit at 1/11/2020.

[8] https://github.com/openssl/openssl . Last visit at 1/11/2020.

[9] https://slproweb.com/download/Win32OpenSSL_Light-1_1_0d.exe. Last visit at 1/11/2020.

[10] GOBI, M.; SRIDEVI, R. and PRIYADHARSHINI, R., *A Comparative Study on the Performance and the Security of RSA and ECC Algorithm*. International Journal Of Advanced Networking and Applications (IJANA),2015, PP.168-171

[11] NISHA, SH. and FARIK, M., *RSA Public Key Cryptography Algorithm–A Review*. International Journal of Scientific & Technology Research, 2017, Vol.6, pp. 187-191.

[12] VERMA, SH. and OJHA, D., *Discussion on Elliptic Curve Cryptography and Its Applications*. International Journal of Computer Science Issues, Vol. 9, No. 1, January 2012, pp.74-78.

[13] WOLF, CH., *Introduction to Multivariate Quadratic Public Key Systems and their Applications*, In Proceeding of YACC 2006 – Yet Another Conference on Cryptography, Porquerolles, France, 2006, pp. 44-55.

[14] Jintai, D. and Yang, B., *Multivariate public key cryptography. Post-quantum cryptography*. Springer, Berlin, Heidelberg, 2009, pp.193-241.

[15] GLIGOROSKI, D; MARKOVSKI, S and KNAPSKOG, S. *A Public Key Block Cipher Based on Multivariate Quadratic Quasigroups*, arXiv:0808.0247v1 [cs.CR], Vol. 6, 2 Aug 2008, pp.113-135.

[16] MARKOVSKI, S. and BAKEVA, V., *quasigroup string processing*, Contributions, Section of Natural, Mathematical and Biotechnical Sciences, Vol. 27, No. 1-2, 2017, pp. 41-53.

[17] SHCHERBACOV, V., *Quasigroups in cryptology*. arXiv:1007.3572v1 21 Jul [math.GR], 2010, pp. 2-22.

[18] GLIGOROSKI, D.; KNAPSKOG, S.; MARKOVSKI, S. and et al, *The Digital Signature Scheme MQQ-SIG*. arXiv:1010.3163v1 [cs.CR] , Vol. 4, 15 Oct 2010, pp.85-91.

[19] http://cpham.perso.univ-pau.fr/WSN-MODEL/wvsn.html . Last visit at 1/11/2020.

[20] JBEILY, T.; ALKUBEILY, M. and HATEM, I., *An Efficient Adaptation of Edge Feature-Based Video Processing Algorithm for Wireless Multimedia Sensor Networks*. In International Journal of Computer Science Trends and Technology (IJCST), Vol.3, No.3, 2015, pp. 156-166.

[21] SHIM, K.; PARK, CH. And KOO, N., *An Efficient MQ-Signature scheme Based on Sparse Polynomials*. IEEE, Vol.8, 2020, pp. 26257-26264.