مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (39) العدد (6) 2017
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (39) No. (6) 2017

Performance Evaluation of MQQ-SIG Algorithm in Wireless Multimedia Sensor Networks

Dr. Boushra Maala*
Khadijeh Iskander**

(Received 9 / 4 / 2017. Accepted 2 / 11 / 2017)

□ ABSTRACT □

Wireless multimedia sensor network (WMSN) consists of large number of small size, low power, limited sources sensor nodes, which are deployed in tested field. These nodes have the ability to sense, to process, to store and to send multimedia data from the environment in real time. A security issue in WMSNs is one of important issues that should be study, because of the special nature of this network, and the importance of inquest basic security requirements of sending information in the network. Using digital signature is very effective way to verify source node`s identity, and it is considered as an important way to detect "Man In Middle" attack, and to achieve data integrity and privacy.

MQQ algorithm which is recently proposed is one of public key cryptography (PKC) algorithms. This algorithm provides good performance as other PKC algorithms such as ECC and RSA. In addition, the implementation of digital signature based on MQQ algorithm -which is called MQQ-SIG- has very good advantages when applied to other networks. In this paper, we present an analyzing study of implementation MQQ-SIG in WMSNs. To achieve our goal, we used real images which are taken by multimedia wireless sensor nodes. We studied important parameters such as size of generated keys, execution time and space occupied in flash memory of multimedia wireless sensor nodes.

Results showed that MQQ-SIG has good performance, as well as the short execution time for generating digital signature, and the execution time of signing and verification operations as similar as that of 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، digital signature, MQQ PKC algorithm, quasigroups.

* **Assistant Professor, Department of Communication and Electronics, Factually of Mechanical and Electrical Engineering, Tishreen University, Lattakia, Syria.**
** **Postgraduate Student, Department of Communication and Electronics, Factually of Mechanical and Electrical Engineering, Tishreen University, Lattakia, Syria.**

مجلة جامعة تشرين للبحوث والدراسات العلمية _ سلسلة العلوم الهندسية المجلد (39) العدد (6) 2017
Tishreen University Journal for Research and Scientific Studies - Engineering Sciences Series Vol. (39) No. (6) 2017

تقييم أداء خوارزمية التوقيع الرقمي MQQ–SIG في شبكات الحساسات اللاسلكية الداعمة للوسائط المتعددة

د. بشرى معلا•
خديجة اسكندر ••

(تاريخ الإيداع 9 / 4 / 2017. قُبِل للنشر في 2/ 11 / 2017)

□ ملخّص □

تتكون شبكة الحساسات اللاسلكية الداعمة للوسائط المتعددة (WMSN) من عدد كبير من العقد الحساسة صغيرة الحجم، منخفضة الطاقة، ومحدودة المصادر، يتم نشرها 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 التوقيع الرقمي من أهم الأساليب المُتّبعة للتحقق من هوية العقدة المصدر، ومن أهم الطرائق المستخدمة للحد من هجوم "رجل في المنتصف" وبالنتيجة الحفاظ على خصوصية وتكاملية معطيات الشبكة.

إن خوارزمية MQQ التي اقترحت حديثاً، هي إحدى خوارزميات المفتاح العام PKC. حققت هذه الخوارزمية أداءً جيّداً مقارنةً مع نظيراتها من خوارزميات المفتاح العام الأخرى مثل خوارزميتي RSA و ECC. إضافة إلى ذلك، إن تنفيذ التوقيع الرقمي اعتماداً على خوارزمية MQQ – والذي يُدعى بـ MQQ–SIG – حقق مزايا جيّدة عند تطبيقه على الشبكات الأخرى. نقدّم في هذا البحث دراسة تحليلية لتطبيق MQQ–SIG 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 وزمن التنفيذ والحيز المحجوز من ذاكرة الحساس. أظهرت النتائج أن MQQ–SIG قدم أداءً جيداً، فضلاً عن الزمن القصير لتوليد التوقيع الرقمي، وزمن تنفيذ عملية التوقيع والتحقق المماثل لما هو 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، التوقيع الرقمي، خوارزمية المفتاح العام MQQ ، أشباه الزّمر.

• مدرس، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سورية
•• طالبة ماجستير، قسم هندسة الاتصالات والالكترونيات، كلية الهندسة الميكانيكية والكهربائية، جامعة تشرين، اللاذقية، سورية.

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 عقد 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 [1,2,3].

مع هذا الانتشار الواسع لهذه الشبكات وتنوّع تطبيقاتها، تظهر التحديات الأمنية انطلاقاً من الطبيعة الخاصة لهذه الشبكات، كطبيعة المنطقة التي يتم نشر الحساسات فيها والتي قد يكون من الصعب مراقبتها مباشرة، الطبيعة الفيزيائية للحساسات (سريعة الفشل، غير مقاومة للتلاعب)، والطبولوجيا غير الثابتة (إضافة وإزالة عقد حساسة)، إضافة إلى الثغرات الأمنية الناتجة عن الاتصالات اللاسلكية. يُعدّ هجوم "رجل في المنتصف" من أكثر الاختراقات الأمنية شيوعاً في هذا النوع من الشبكات، وتأتي خطورة هذا الهجوم من كونه يُهدّد سرية وتكاملية المعلومات، إذ يمكن لعقدة مزيّفة أن تخترق الاتصال بين عقدتين من أصل الشبكة وتطلع على محتوى الرسالة، وتقوم بتعديله. 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 التوقيع الرقمي من أكثر الأساليب الأمنية الفعالة للتحقق من هوية العقدة المُرسِلة، ومن أهم طرائق كشف هجوم "رجل في المنتصف" وبالنتيجة الحفاظ على خصوصية وتكاملية معطيات الشبكة [4,5,6].

ظهرت مؤخّراً خوارزمية المفتاح العام(Multivariate Quadratic Quasigroup) MQQ، وهي إحدى خوارزميات المفتاح العام المعتمدة على كثيرات الحدود التربيعية متعددة المتحوّلات MQPKC (Multivariate Quadratic Public Key Cryptosystems)، يتميز هذا النوع من الخوارزميات بسرعته في توليد التواقيع الرقمية [7,8].

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 و طبيعة الاتصال اللاسلكي، كل ذلك يجعل اختراق هذه الشبكات وتهديد أمنها أمراً ممكناً. وعلى الرغم من أنّ التشفير يمنع غير المخول لهم من الاطلاع على محتوى الرسالة، إلّا أنّه لا يمنع المخربين من العبث بمحتواها، ومن هنا ظهرت الحاجة إلى التوقيع الرقمي والذي يُعدّ من أكثر الأساليب الأمنية المُتّبعة للتحقق من هوية العقدة المُرسِلة، ومن أهم طرائق التصدي لهجوم "رجل في المنتصف" وبالنتيجة الحفاظ على خصوصية وتكاملية معطيات الشبكة [9,10].

يهدف هذا البحث إلى التعرّف على خوارزمية المفتاح العام MQQ وبارامتراتها، ودراسة تطبيق التوقيع الرقمي MQQ–SIG في شبكات الـ WMSNs للتحقق من تكاملية وسلامة الرسالة، ومن ثمّ تقييم أداء هذا التوقيع الرقمي المولد باستخدام MQQ–SIG من خلال مقارنته مع التوقيع الرقمي باستخدام خوارزمية RSA الشهيرة.

طرائق البحث ومواده:

تمّت برمجة جميع مراحل خوارزمية MQQ–SIG بلغة C وتم تنفيذها وتطبيقها باستخدام برنامج (Code::Blocks /version 16.01/) وهو عبارة عن مترجم خاص بلغة (C/C++)، بالإضافة إلى عملية ربط المترجم بالمكتبة (GNU) والتي تعد بمثابة مكتبة عددية مفتوحة المصدر خاصة بلغة (C /C++)، تزود بدورها توابع رياضية ومولدات أعداد عشوائية وغير ذلك من التطبيقات التي تستخدم على نطاق واسع من قبل الأنظمة مفتوحة المصدر لإنجاز العمليات الحسابية.

تمت المقارنة مع خوارزمية المفتاح العام RSA مكتوبة بلغة البرمجة C والمضمنة في مكتبة openssl [11]، وهي عبارة عن مكتبة مفتوحة المصدر تحتوي على أدوات التشفير وتستعمل بروتوكولات طبقة النقل الآمن، وتقوم بتنفيذ المهام الأساسية للتشفير وتوفر وظائف مختلفة. يمكن استخدام openssl في مجموعة متنوعة من لغات البرمجة، وإصدارات متاحة لمعظم أنظمة التشغيل. تمّ تنفيذ مراحل خوارزمية RSA (توليد المفاتيح، التوقيع الرقمي، والتحقق) باستخدام برنامج win32openssl 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 Diffie – DH (Hellman) التي تعتمد على صعوبة حل اللوغاريتمات المتقطعة، وتمّ استخدامها 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 [12,13,14].

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 [7,8,15,16].

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

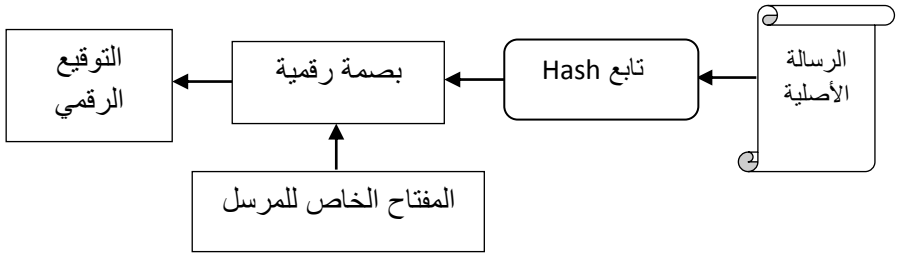
1.1 التوقيع الرقمي Digital signature :

يمثل التوقيع الرقمي بصمة رقمية للرسالة يتم اشتقاقها من الرسالة ذاتها وفقاً لخوارزميات معينة تقوم بتطبيق حسابات رياضية على الرسالة لتوليد هذه البصمة الالكترونية.

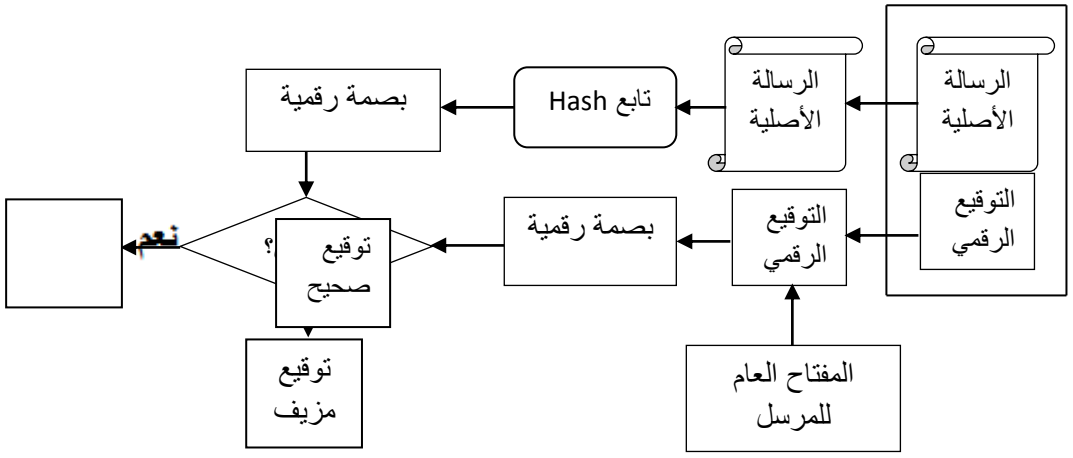
يتكون التوقيع الرقمي للرسالة من بيانات لها طول ثابت تؤخذ من الرسالة ذات الطول المتغيّر. يستطيع هذا التوقيع تمييز الرسالة الأصليّة والتعرّف عليها بدقة، حيث أنّ أي تغيير في الرسالة ـ ولو كان بتاً واحداً ـ سيعطي توقيعاً رقمياً مختلفاً تماماً، بهذا سيكون من غير الممكن اشتقاق التوقيع الرقمي ذاته من رسالتين مختلفتين. فهو بذلك يشكل وسيلة أمنية فعّالة لضمان تكاملية معطيات الرسالة.

يقوم المرسل بتوليد التوقيع الرقمي للرسالة باستخدام المفتاح الخاص، أمَّا المستقبل فيتحقق من صحة التوقيع عن طريق استخدام المفتاح العام المطابق، وبذلك يمنع التوقيع الرقمي المرسل من التنكّر للمعلومات التي أرسلها كونه الوحيد الذي يملك المفتاح الخاص أي يُحدّد هوية المرسل، وهذا بدوره يضمن تحقيق متطلب المصادقة أيضاً [17].

ويوضح الشكلين الآتيين كل من آليتي توليد التوقيع الرقمي والتحقق منه:



الشكل (1) : مخطط توضيحي لآلية التوقيع الرقمي



الشكل (2) : مخطط توضيحي لآلية التحقق من صحة التوقيع الرقمي

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

تُعدّ خوارزمية تشفير المفتاح العام المعتمدة على أشباه الزّمر التربيعية متعددة المتحوّلات MQQ (Multivariate 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 [18,19,20].

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، نقوم بتمثيلها كتوابع بوليانية vector valued Boolean functions (v.v.b.f)، ولهذا نختار تابع تقابلي (bijection) $\beta: Q \to \{0,1, \dots\dots, 2^d - 1\}$ ، حيث يتم تمثيل كل عنصر $a \in Q$ بسلسلة فريدة من البتات $(x_1, x_2, \dots\dots, x_d) \in \{0,1\}$.

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

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

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

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 (algebraic normal form) وفق القانون الآتي :

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

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 $M = a_1 a_2 \dots\dots a_n$

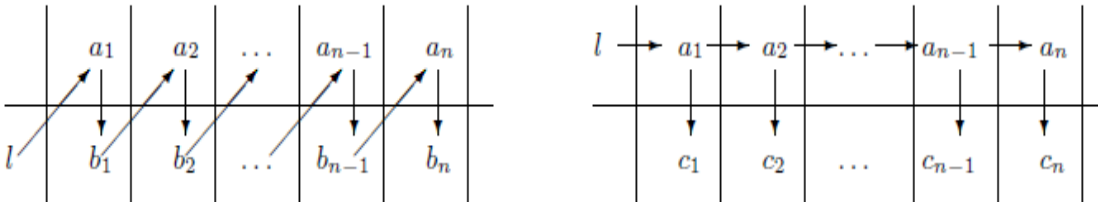
حيث أنّ $a_i \in Q$ ، و بفرض لدينا العنصر القائد (leader) هو $l \in Q$ ، فإنّ هناك تحويلين أساسيين هما

: d− transformation و e−transformation

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

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

ويبين الشكل (3) مخطط لتحويلي e و d :



الشكل (3) : تحويلا e و d

أشباه الزّمر التربيعية متعددة المتحوّلات :

عموماً عند توليد أشباه زمر بشكل عشوائي بعامل 2^d حيث $4 \leq d$ ، 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 $0 \leq k < d$.

يمكن وصف عملية توليد أشباه الزمرة التربيعية متعددة المتحولات MQQs وفق المعادلة الآتية [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 B , A_2 , A_1 هي مصفوفات قابلة للعكس وكل منها بحجم $d \times d$ ويتم توليد عناصرها بشكل عشوائي في$GF(2)$. و الشعاع C بطول d وعناصره يتم توليدها 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:

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

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

عندئذٍ سنحصل على أشباه الزّمر

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

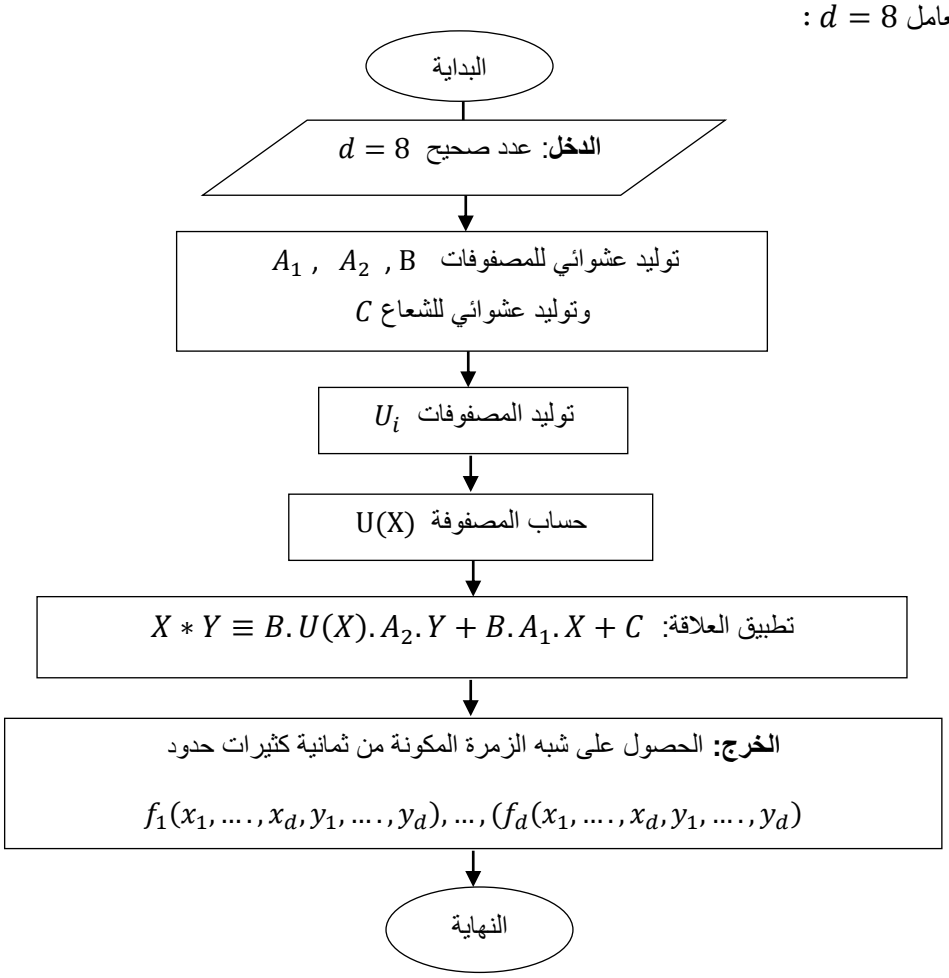
سنهتم منها فقط بأشباه الزّمر التي تحقق الشرط الآتي:

$$Rank\left(B_{f_i}\right) \geq 2d - 4$$

حيث أنّ المصفوفات B_{f_i} هي مصفوفات بوليانية وكل منها بحجم $2d \times 2d$ ويتم إيجادها وفق الآتي :

$$B_{f_i} = \left[b_{j,k}\right], b_{j,8+k} = \ b_{8+k,j} = 1 \quad (10)$$

إذا كان $x_j y_k$ هو جزء من f_i. ويبين المخطط الآتي خطوات توليد شبه الزمرة MQQ من أجل العامل $d = 8$:



الشكل (4) : مخطط توليد شبه الزمرة بعامل $\mathbf{d = 8}$

2. التوقيع الرقمي MQQ–SIG :

يُعطى الشكل العام لمخطط التوقيع الرقمي MQQ–SIG 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)

–الشعاع v بولياني طوله n بت.

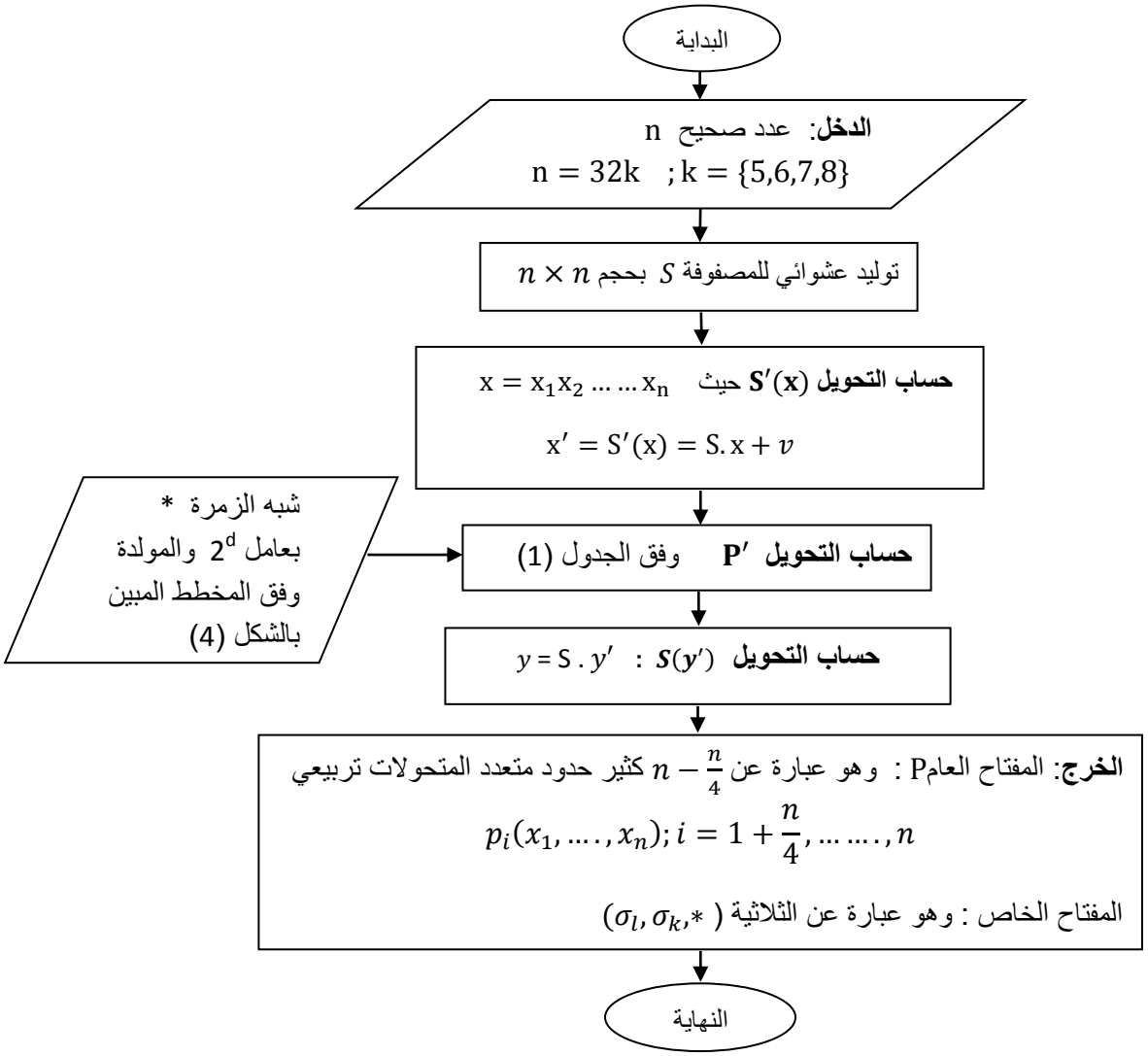
$$v = (v_1, v_2, \dots \dots, v_n) \; ; \; v_i = \left(\frac{S^{(k)}_{\lceil i/4 \rceil}}{2^{i \bmod 4}} \right) \bmod 2 \qquad (11)$$

يبين الجدول (1) وصفاً للتحويل المركزي P':

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

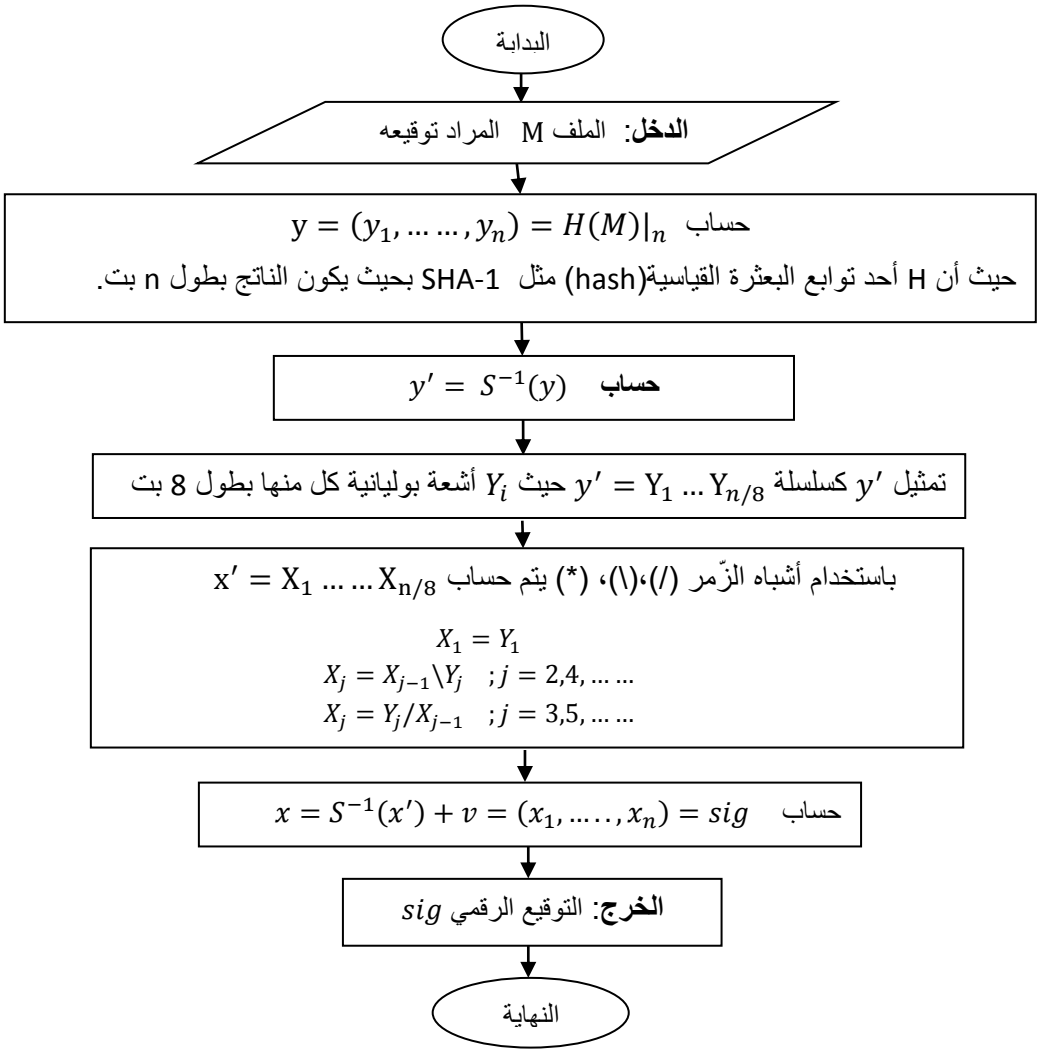
الدخل: الشعاع $x' = (f_1, \dots\dots, f_n)$ والذي يتألف من n تابع خطّي وكل منها تابع لـ n متحوّل $n = 32k \quad ; k = 5,6,7,8$
الخرج: y' ومؤلف من 8 توابع خطية $P_i'(x_1, \dots\dots, x_n)\ , i = 1, \dots\dots, 8$ و $8-n$ كثير حدود تربيعي متعدد المتحولات $P_i'(x_1, \dots\dots, x_n), i = 9, \dots\dots, n$
الخطوات: 1. تمثيل الشعاع $x' = f_1 .. f_n$ كسلسلة $x' = X_1 X_2 \dots X_{n/8}$ ، حيث X_i أشعة كل منها بطول 8 بت 2. حساب $y' = Y_1 Y_2 \dots\dots Y_{n/8}$ حيث : $Y_1 = X_1$ من أجل الأعداد الزوجية .. $j = 2,4,\dots$ $Y_{j+1} = X_j * X_{j+1}$ من أجل الأعداد الفردية ... $j = 3,5,\dots$ $Y_{j+1} = X_{j+1} * X_j$

يبين المخطط الآتي آلية توليد زوج المفاتيح (عام & خاص) وفق خوارزمية MQQ [21]:



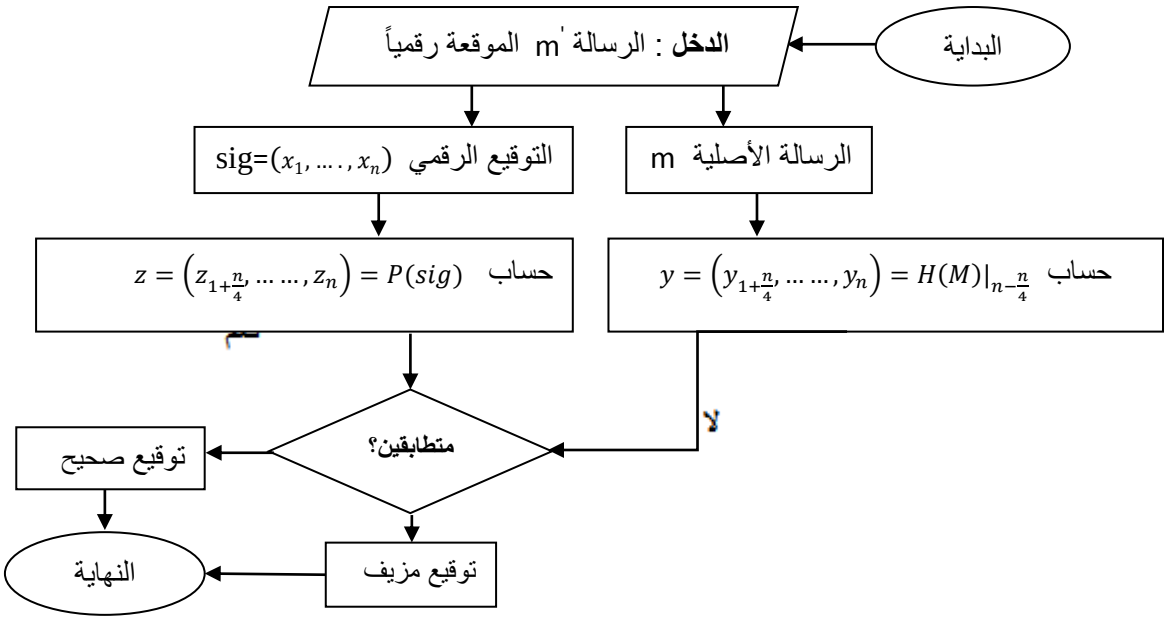
الشكل (5) : مخطط توليد زوج المفاتيح (عام & خاص) وفق خوارزمية MQQ

– تتم عملية التوقيع الرقمي MQQ–SIG باستخدام المفتاح الخاص وفق الخوارزمية المبينة في الشكل الآتي[21]:



الشكل (6) : مخطط عملية التوقيع الرقمي *MQQ–SIG* باستخدام المفتاح الخاص

أما عملية التحقق من صحة التوقيع الرقمي باستخدام المفتاح العام فتتم وفق المخطط المبين في الشكل الآتي[21].



الشكل (7) : آلية التحقق من صحة التوقيع الرقمي MQQ-SIG

خوارزمية RSA :

تعد خوارزمية RSA أوّل خوارزمية تشفير غير متناظر والتي تم نشرها 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 [13]. يتم توليد زوج المفاتيح (عام &خاص) وفق خوارزمية RSA من خلال الخطوات الآتية:

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

2- حساب $\boldsymbol{n = p \times q}$

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

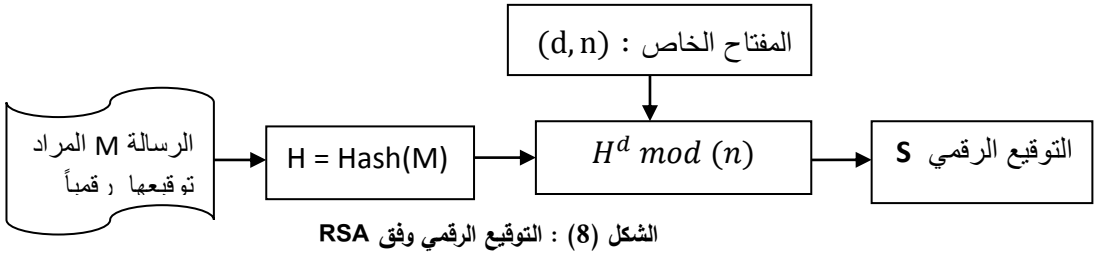
4- اختيار العامل e بحيث تحقق العلاقة الآتية: $1 < e < \varphi(n)$

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

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

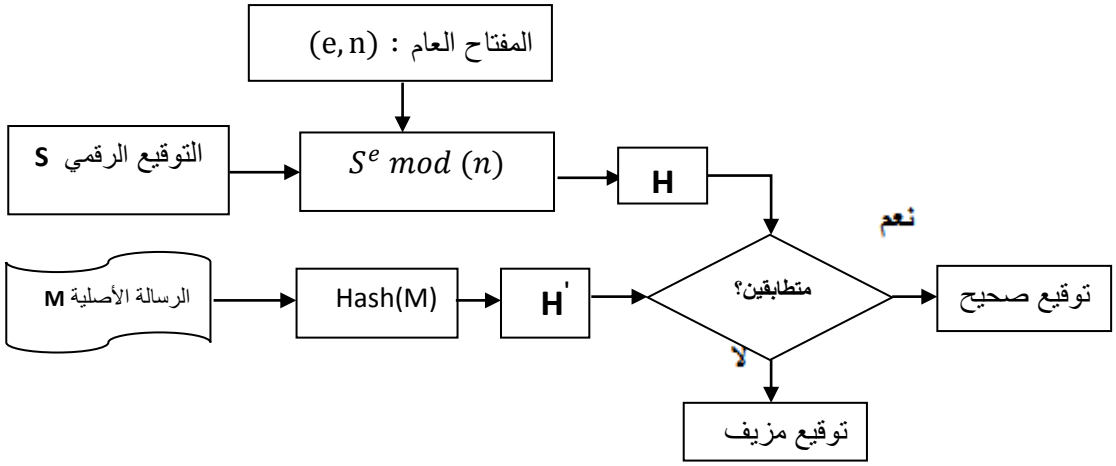
نحصل بذلك على زوج المفاتيح : المفتاح العام : (e, n) ، المفتاح الخاص : (d, n)

تتم عملية التوقيع الرقمي وفق خوارزمية RSA باستخدام المفتاح الخاص كما هو موضح في الشكل (8).



الشكل (8) : التوقيع الرقمي وفق RSA

أما عملية التحقق من صحة التوقيع الرقمي باستخدام المفتاح العام تتم وفق الشكل الآتي :



الشكل (9) : التحقق من صحة التوقيع الرقمي وفق RSA

النتائج والمناقشة:

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

الشكل (10) : نموذجي الصور المستخدمة في عملية المحاكاة

تُعدّ هذه الصور من أشهر صور الحساسات اللاسلكية المستخدمة كنماذج اختبارية في الأبحاث العلمية [22]. تمّ تطبيق خوارزمية المفتاح العام MQQ-SIG المدروسة آنفاً على نموذجي الصور المختارة، وتمّ اختبار هذه الخوارزمية ومقارنتها مع خوارزمية المفتاح العام الشهيرة RSA عند تطبيقها على نفس الصور.

وتمّ التنفيذ على جهاز حاسب ذو مواصفات مبينة 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

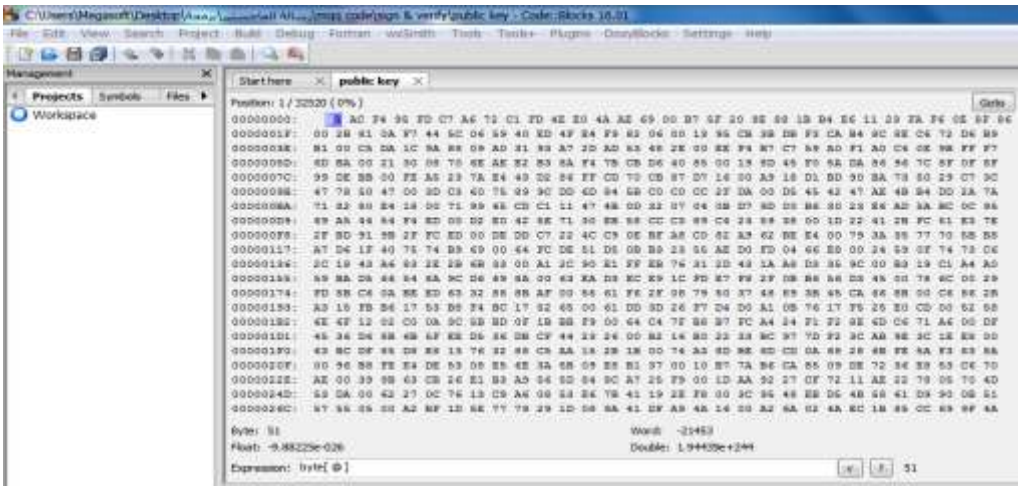
اعتمدنا في عملية التحليل والمقارنة على مجموعة من البارامترات الهامة لتقييم الأداء وهي: أحجام المفاتيح المولّدة، وسرعة التنفيذ، والحيز المحجوز من ذاكرة الحساس اللاسلكي.

1.4 سيناريو العمل:

السيناريو الأول : قمنا بتطبيق خوارزمية التوقيع الرقمي MQQ-SIG بمراحلها الثلاثة (توليد المفاتيح، التوقيع، التحقق) على نموذجي الصور المختارة للدراسة وذلك من أجل n=160.

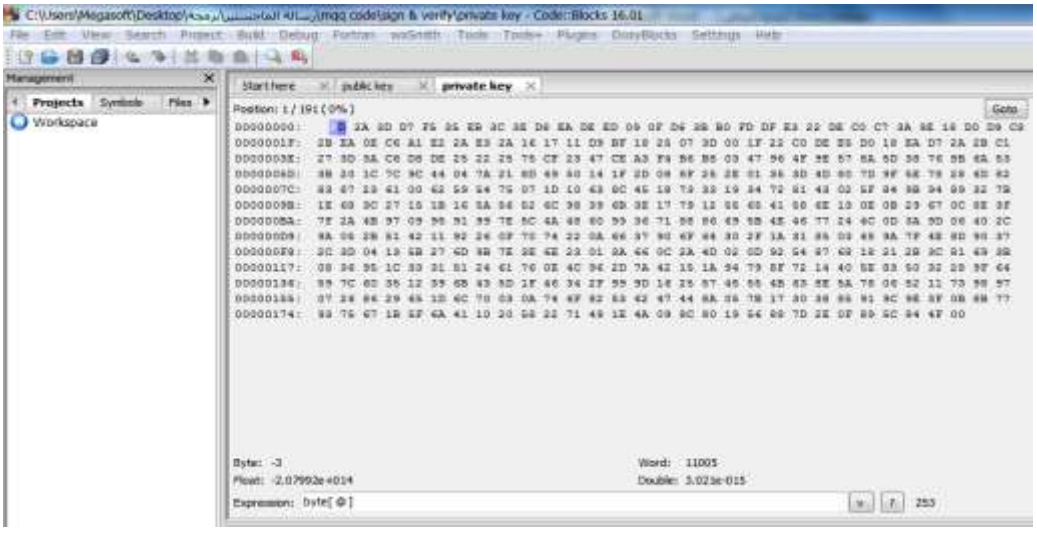
أوّلاً: توليد المفاتيح : تمّ توليد زوج المفاتيح (عام & خاص) وفق الخوارزمية الموضّحة في الشكل رقم (5).

حصلنا عند التنفيذ على المفتاح العام، ويبين الشكل الآتي جزء من هذا المفتاح العام بالترميز الست عشري، تعذّر عرضه بشكل كامل لكبر حجمه.



الشكل (11) : جزء من المفتاح العام الناتج وفق MQQ

وحصلنا على المفتاح الخاص الموافق والمبيّن في الشكل الآتي بالترميز الست عشري:



الشكل (12) : المفتاح الخاص الناتج وفق MQQ

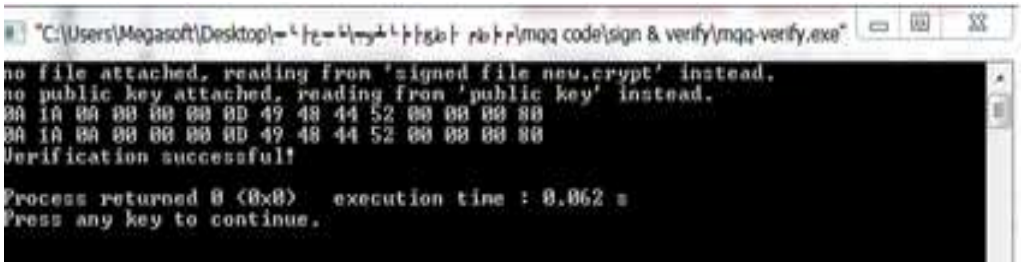
ثانياً: التوقيع الرقمي : تمّ توقيع الصور المدروسة رقميّاً وفق المخطط الموضح في الشكل (6) وحصلنا على النتائج الآتية:

الجدول (3) : نتائج التوقيع الرقمي MQQ–SIG

الصورة المدروسة	التوقيع الرقمي بطول 160 bit
الصورة الأولى بحجم 29.3KB	6F 8C 6B 07 E8 40 C6 29 04 C5 B6 15 BD 72 1D 9C 96 DC 8D F9
الصورة الثانية بحجم 268KB	2F 9D E6 81 21 12 D9 3A 0D 2B C5 15 88 96 C0 64 AD 49 14 2B

ثالثاً: التحقق:

تمّ التحقق من صحّة التوقيع الرقمي وفق المخطط رقم (7) وكانت النتيجة كالآتي :

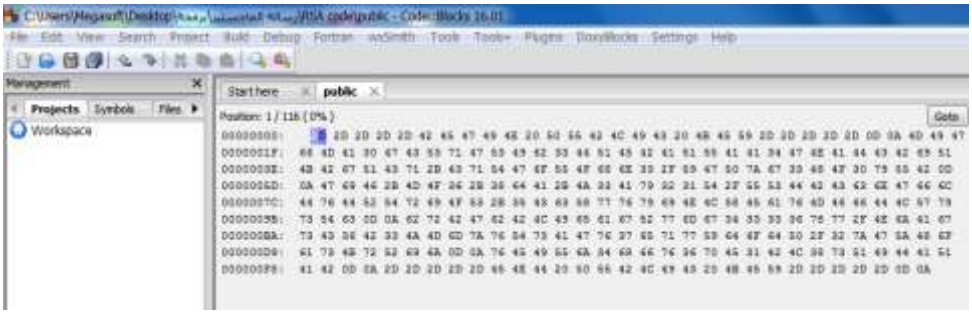


الشكل (13) : يبين نتيجة التحقق من صحة التوقيع الرقمي MQQ–SIG للصورتين

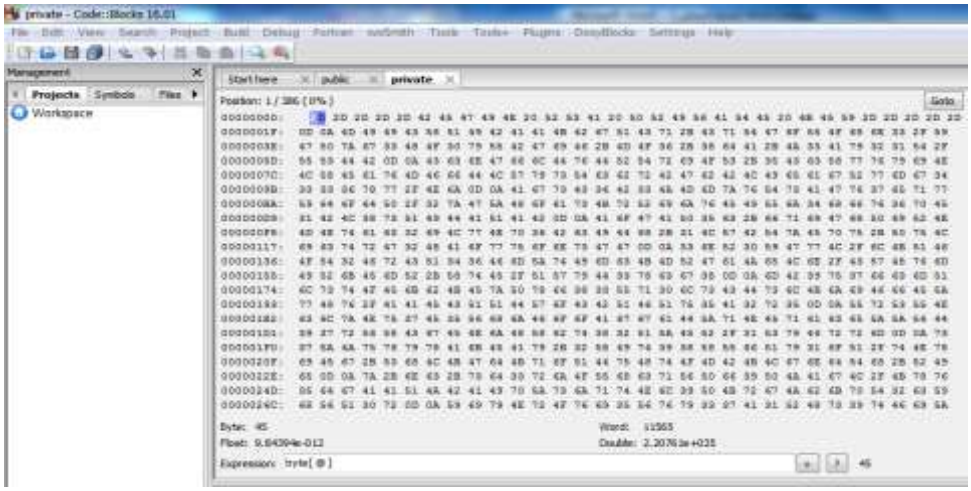
السيناريو الثاني:

تحقق خوارزمية RSA–1024 نفس مستوى الأمن الذي تحققه خوارزمية MQQ–160 [23]. قمنا في هذا السيناريو بتطبيق خوارزمية المفتاح العام الشهيرة RSA وذلك من أجل n=1024 على نموذجي الصور المدروسة، علماً أنّ تابع الـ hash المستخدم في الخوارزمية هو SHA–256 .

أوّلاً: توليد المفاتيح : تمّ توليد زوج المفاتيح (عام & خاص) وفق خوارزمية RSA المشروحة سابقاً وحصلنا على المفاتيح المطلوبة والمبينة في الشكلين الآتيين :



الشكل (14) : المفتاح العام وفق خوارزمية RSA–1024



الشكل (15) : المفتاح الخاص وفق خوارزمية RSA-1024

ثانياً: التوقيع: تمّ توقيع الصور المدروسة رقميّاً وفق خوارزمية RSA-1024 وحصلنا على النتائج الآتية:

الجدول (4) : نتائج التوقيع الرقمي RSA-1024

الصورة المدروسة	التوقيع الرقمي بطول 1024 bit
الصورة الأولى بحجم 29.3KB	3D A8 40 28 D1 67 57 D4 41 9F 96 D6 31 BE 30 04 AF F1 B1 AF 54 C9 04 44 EB F1 55 F7 8A A7 8E 68 AB B1 DA 75 D3 EF 0D B2 F6 E5 E9 A0 B4 9D 1D E0 82 BB 97 CB 4F 32 F1 18 A1 26 66 66 29 0B B8 B1 66 42 B4 2B 61 8F 5A FB 83 56 B9 7B 85 1F 72 2B 0B 7C A3 15 C5 6F F2 D5 6A 3D 60 BE 81 46 79 A1 81 00 50 25 6D 5E 4A 62 68 DF 77 70 35 41 C0 56 37 D5 C1 F6 59 D8 BB BE B9 7A 4E F8 E0 25 1F B3
الصورة الثانية بحجم 268KB	99 86 BC B4 75 19 C0 E7 F9 02 6B C5 CC 24 4E 53 18 5E 73 0E DC 48 9A 45 3E A5 A5 7A 41 D8 E5 67 48 3C 5D 96 1F 51 10 95 B1 B7 78 3C 18 0D FE E9 D0 AE 9A ED 33 9C 0E A5 74 E7 86 26 48 26 57 18 9D C2 03 A1 9D 8C 9C A7 12 A7 17 26 E3 EF F6 57 C6 57 31 9D D5 E1 11 D9 8A C3 06 11 1E D1 26 A8 80 26 BA D7 FB 7A 0D 30 49 E2 9F 64 8D B3 A8 5B 88 DB 87 4B C5 60 2A 2E 70 21 0C 10 A9 71 95 1B

قمنا أخيراً بالتحقق من صحّة التوقيع الرقمي باستخدام RSA-1024 وفق المخطط المبين في الشكل (9) .

مناقشة النتائج:

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

1- مستوى الأمن المحقق :

مستوى الأمن المحقق بواسطة خوارزمية MQQ–SIG هو ($2^{\frac{n}{2}}$) وبالتالي من أجل n=160 يكون مستوى الأمن المحقق هو 2^{80}، تعطي خوارزمية RSA–1024 نفس مستوى الأمن الذي تعطيه خوارزمية MQQ–160

ذكرنا سابقاً أنّ خوارزمية RSA تعتمد في تحقيق أمنها على صعوبة تحليل أعداد أوّلية كبيرة إلى عواملها الأوّلية، وبالتالي من أجل $n = 1024$ bit يزداد التعقيد الحسابي للخوارزمية والناتج عن كون العددين الأوليين p , q يجب أن يكونا كبيرين لأنّ $\boldsymbol{n = p \times q}$ ، بالإضافة 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 تعقيد حسابي وأكثر بساطة وأسرع في التنفيذ من التوابع المستخدمة في خوارزمية RSA.

2- أحجام المفاتيح والتوقيع الرقمي:

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.

حسب الخوارزمية المدروسة في هذه المقالة فإنّه تمّ تخفيض حجم المفتاح العام إلى $n - \frac{n}{4}$ معادلة تربيعية متعددة المتحولات، وبالتالي يُعطى حجم المفتاح العام بالعلاقة الآتية:

$$0.75 \times n \times \frac{1+\frac{n(n+1)}{2}}{8\times 1024} \quad KByte \qquad (12)$$

أمّا المفتاح الخاص وفق خوارزمية MQQ فيتألف من شبه الزّمرة التربيعية المولّدة بعامل 2^8 ممثلة بـ 81 Byte ، بالإضافة للمصفوفة S البوليانية والتي تمّ تمثيلها بطريقة معينة ليكون حجمها 2n Byte ، وبالتالي يُعطى حجم المفتاح الخاص حسب العلاقة الآتية:

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

يبيّن الجدول الآتي أحجام المفاتيح والتواقيع الرقمية التي حصلنا عليها لدى تطبيق خوارزمية MQQ من أجل $n = 160$ و خوارزمية RSA من أجل $n = 1024$:

الجدول (5) : أحجام المفاتيح والتوقيع الرقمي الناتجة

الخوارزمية	المفتاح العام	المفتاح الخاص	التوقيع الرقمي
MQQ–160	188.685 Kbyte	401 Byte	160 bit
RSA–1024	278 Byte	902 Byte	1024bit

نلاحظ من الجدول السابق أنّ حجم المفتاح العام وفق MQQ يعادل تقريباً 10^3 من حجم المفتاح العام وفق RSA ، أما حجم المفتاح الخاص وفق MQQ فهو تقريباً نصف حجم المفتاح الخاص وفق RSA. إنّ الحجم الكبير للمفتاح العام لخوارزمية MQQ يزيد من صعوبة كسر هذه الخوارزمية، وهذا ناتج عن صعوبة حلّ معادلات غير خطّية في الحقول المنتهية وهذا ما يُسمّى بـ MQ–problem ، إذ أنّ حل $n - \frac{n}{4}$ معادلة غير خطّية يتطلّب زمن كبير جدّاً وهذا ما يُعرف بـ NP–hardness problems (non–deterministic polynomial–time hard) ولكن من ناحية أخرى يُعدّ الحجم الكبير للمفتاح العام نقطة مهمّة جدّاً يجب أخذها بعين الاعتبار عند تطبيق هذه الخوارزمية، لأنّ هذا سيتطلّب حيّز من الذاكرة أكبر بكثير من الحيّز اللازم لتخزين المفتاح العام في خوارزمية RSA .

من أجل نفس مستوى الأمن نلاحظ أنّ MQQ قد وقّعت رقميّاً الصورة بـ 160bits، بينما RSA وقعت نفس الصورة بـ 1024bits. وبما أنّ هذا التوقيع الرقمي سيتم إرساله مع الرسالة الأصلية من العقدة المصدر إلى العقدة الهدف، فإنّ الحجم الصغير للتواقيع الرقمية الناتجة وفق خوارزمية MQQ يُعدّ ميّزة مهمّة لهذه الخوارزمية مقارنة بخوارزمية RSA .

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

تمّ تطبيق كل من خوارزميتي المفتاح العام MQQ-160 و RSA-1024 بمراحلهما الثلاثة (توليد المفاتيح، التوقيع الرقمي، التحقق من صحة التوقيع) على نموذجي الصور المقترحة، وتمّ التنفيذ على جهاز حاسوب بالمواصفات المذكورة سابقاً، قمنا بقياس الزمن الذي تحتاجه كل خوارزمية لإنجاز كل مرحلة. تمّ التنفيذ عدّة مرّات ثم أخذ المتوسط الحسابي للزمن اللازم مقدّراً بالثانية، ويبيّن الجدول الآتي النتائج التي حصلنا عليها:

الجدول(6) : سرعة عملية التنفيذ مقدرة بالثانية

الخوارزمية	توليد المفاتيح	الصورة الأولى بحجم 29.3KB		الصورة الثانية بحجم 268KB	
		التوقيع	التحقق	التوقيع	التحقق
MQQ-160	0.226	0.1154	0.0682	0.0988	0.0462
RSA-1024	0.25	0.092	0.05	0.06	0.066

نلاحظ من الجدول السابق أنّ خوارزمية المفتاح العام MQQ تحقق أداء جيّداً من ناحية سرعة تنفيذ العمليّات، فهي تحتاج لأجزاء من الثانية لإنجاز كل مرحلة، وهذا يُعدّ ميّزة هامّة لهذه الخوارزمية عند تطبيقها في شبكات الـ WMSNs ، إذ أنّ سرعة تنفيذ خوارزمية MQQ-160 تقارب تماماً سرعة تنفيذ خوارزمية RSA-1024 الشهيرة. نلاحظ أيضاً أنّ حجم الصورة لم يؤثّر كثيراً على أداء الخوارزمية، إذ أنّ سرعة تنفيذ الخوارزمية عند تطبيقها على الصورة الأولى قد بقي تقريباً كما هو عند تطبيقها على الصورة الثانية والتي يبلغ حجمها حوالي 9 أضعاف الصورة الأولى.

4- الحيّز المحجوز من ذاكرة الحسّاس اللاسلكي :

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

شملت الدراسة عدّة نماذج مبيّنة في الجدول الآتي مع الذواكر المتاحة ضمن كل عقدة حساس[24].

الجدول (7) :بعض مواصفات نماذج العقد الحساسة المستخدمة في الدراسة

العقدة الحساسة	المعالج	الذاكرة
Imote2	Intel PXA271 XScale® Processor at 13 – 416MHz	32MB Flash 256 KB SRAM 32 MB SDRAM
Mesheye	ARM7TDMI- ARM thumb processor. at up to 47.92 MHz.	256 KB Flash 64 KB SRAM
CSIRO fleckTM-3	ADSPBF537 Blackfin processor at 600 MHz.	1 MB Flash 8 KB RAM
Netbook	Intel Atom N270 single core at 1.6 GHz	8 GB Flash 512 MB RAM

على اعتبار أنه يتم تخزين زوج المفاتيح (عام & خاص) ضمن ذاكرة الـ flash لعقدة الحساس، إنّ الحجم اللازم لتحزين زوج المفاتيح هو حجم المفتاح العام + حجم المفتاح الخاص ويساوي:

188685+401=189086Byte

يبين الجدول الآتي النسبة المئوية للحيز المحجوز من ذاكرة flash للعقدة واللازم لتخزين زوج المفاتيح المولّدة وفق خوارزمية MQQ.

الجدول(8) : النسبة المئوية للحيز المحجوز من ذاكرة flash

العقدة الحساسة	Imote2	Mesheye	CSIRO fleckTM-3	Netbook
النسبة المئوية	0.59%	73.86%	18.90%	0.0236%

نلاحظ من الجدول السابق أنّ الحجم اللازم لتخزين المفاتيح أصغريّاً في كل من النموذجين Imote2 و Netbook ، بينما يظهر تأثير الحجم الكبير للمفتاح العام بالنسبة للنموذج CSIRO fleckTM-3 ، إذ يتطلّب تقريباً خمس ذاكرة الـ flash، 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 الحساسات اللاسلكية الداعمة للوسائط المتعددة، إذ يجب اختيار النوع المناسب من العقد الحساسة.

الاستنتاجات والتوصيات:

قمنا في هذا البحث بدراسة خوارزمية المفتاح العام MQQ ، وتطبيق التوقيع الرقمي MQQ-SIG من أجل n=160 لتوقيع صور ملتقطة بواسطة عقدة حساس لاسلكي، وذلك لدراسة مدى فعالية تطبيق هذه الخوارزمية في شبكات الحساسات اللاسلكية الداعمة للوسائط المتعددة.

تبين لنا من خلال الدراسة ومناقشة النتائج 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:

- أظهرت الخوارزمية فعاليتها في توليد تواقيع رقمية قصيرة، كما أظهرت سرعة عالية في تنفيذ العمليات (توليد مفاتيح، توقيع، تحقق) تقارب سرعة خوارزمية RSA، وهذا ناتج عن كونها تعتمد في أساس عملها على عمليات XOR و AND وهي عمليات منطقية بسيطة لا تتطلّب معالجة حسابية عالية ويتمّ إنجازها بسرعة كبيرة، إذ تمكنت الخوارزمية من التوقيع الرقمي لصور بأحجام متفاوتة والتحقق من صحة هذا التوقيع خلال أجزاء من الثانية، فهي بذلك تناسب شبكات الحساسات اللاسلكية الداعمة للوسائط المتعددة التي تتطلب في العديد من التطبيقات سرعة عالية في التنفيذ والإرسال في الزمن الحقيقي.
- 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 الأخذ بالحسبان نوع العقد الحسّاسة المستخدمة والسعات التخزينية المتاحة فيها، وبالتالي مدى إمكانية ملاءمتها لتطبيق خوارزمية المفتاح العام MQQ.

- إنّ الخوارزمية المدروسة في هذا البحث تمّ تطبيقها 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، 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. إضافة إلى دراسة طرائق أخرى لتوليد أشباه الزّمر بسرعة وكفاءة عالية.

المراجع:

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

[2] ATIF, S.; VIDYASAGAR, P. and ELIZABETH, C., *Wireless Multimedia Sensor Network Technology :A Survey*. 7th IEEE International Conference on Industrial Informatics (INDIN) IEEE, 2009, pp.606-613.

[3] PRABHU, T.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,2009.

[5] RACHEDI, A. ; KADDAR, L. and MEHAOUA, A., *EDES- Efficient Dynamic Selective Encryption Framework to Secure Multimedia Traffic in Wireless Sensor Networks*. IEEE ICC'2012, Ottawa, Ontario : Canada, 2012.

[6] KHALIFA,N. ; TAHA,M. and ELMAHDY,H. , *A Secure Energy Efficient Schema for Wireless Multimedia Sensor Networks*. CIIT International of wireless communication, Vol. 5, No. 6, 2013, pp.235-246.

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

[8] SAKUMOTO,K.; SHIRAI,T. and HIWATARI,H., *Public-Key Identification Schemes based on Multivariate Quadratic Polynomials*. Tokyo, Japan Sony Corporation@CRYPTO, 2011.

[9] SEN,J. *A Survey on Wireless Sensor Network Security*. International Journal of Communication Networks and Information Security (IJCNIS), Vol. 1, No. 2, August 2009, pp.55-78.

[10] HARJITO,B. and HAN,S., *Wireless Multimedia Sensor Networks Applications and Security Challenges.* International Conference on Broadband, Wireless Computing, Communication and Applications, 2010.

[11] https://github.com/openssl/openssl . Last visit at 5/4/2017.

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

[13] KAK,A., *Computer and Network Security, Lecture 12: Public-Key Cryptography and the RSA Algorithm.* Purdue University,2016.

[14] KAK,A., *Computer and Network Security, Lecture 14: Elliptic Curve Cryptography and Digital Rights Management.* Purdue University,2017.

[15] WOLF,CH., *Introduction to Multivariate Quadratic Public Key Systems and their Applications*. Ecole Normale Sup´erieure, D´epartement d'Informatique 45 rue d'Ulm , F-75230 Paris Cedex 05, France, Mars 22, 2006.

[16] CARLOS,G., *Introduction to Multivariate Public Key Cryptography*. LARC - Computer Architecture and Networking Lab Department of Computer Engineering and Digital Systems Escola Politécnica University of SaPaulo.2011.

[17] KERRY,C. and GALLAGHER, P., *Digital Signature Standard (DSS).* FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, July 2013.

[18] GLIGOROSKI,D; MARKOVSKI,S and KNAPSKOG, S. *A Public Key Block Cipher Based on Multivariate Quadratic Quasigroups*, arXiv:0808.0247v1 [cs.CR], 2 Aug 2008.

[19] GLIGOROSKI,D; MARKOVSKI,S and BAKEVA,V., *quasigroup string processing,* Maced. Acad. of Sci. and Arts, Sc. Math. Tech. Scien. XX 1-2 , 1999,PP.13-28.

[20] SHCHERBACOV, V., *Quasigroups in cryptology.* arXiv:1007.3572v1 21 Jul [math.GR], 2010.

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

[22] http://cpham.perso.univ-pau.fr/WSN-MODEL/wvsn.html . Last visit at 5/4/2017.

[23] SOOMRO,K., *RFID implementation and performance analysis of a short MQQ digital signature.* Norwegian University of Science and Technology Department of Telematics, June 2010.

[24] FAROOQ,M. and KUNZ, T., *Wireless Sensor Networks Testbeds and State-of-the-ArtMultimedia Sensor Nodes*. Applied Mathematics & Information Sciences, VOL.8, No. 3, 2014, PP.935-940.