التشفير ما بعد الكوانتم: لماذا ينبغي أن نستعد اليوم لخطرٍ لم يقع بعد؟

الهادي خمري
أستاذ باحث، المدرسة الوطنية العليا للتكنولوجيات المتقدمة
elhadi.khoumeri@ensta.edu.dz

يعالج هذا المقال سؤالًا بسيطًا في ظاهره وعميقًا في نتائجه: كيف نحمي بياناتنا الرقمية في المستقبل إذا أصبحت بعض أدوات الحماية المعتمدة اليوم أقلّ صمودًا أمام تطور الحوسبة الكوانتية؟

1. مقدمة

لم تعد حماية البيانات في العصر الرقمي شأنًا تقنيًا يخص المختبرات أو فرق الأمن السيبراني وحدها، بل أصبحت جزءًا من الحياة اليومية للأفراد والمؤسسات والدول. فالمعاملات البنكية، والسجلات الطبية، والمنصات الجامعية، والبريد الإلكتروني، والتوقيع الرقمي، والخدمات الإدارية عن بُعد، كلها تعتمد على طبقة غير مرئية من الثقة تسمى التشفير. وحين يضغط المستخدِم على زر الإرسال أو يدخل كلمة مروره أو يوقع وثيقة رقمية، فإنه يفترض ضمنيًا أن هناك بنية رياضية وتقنية تحمي ما يفعله من التلاعب أو التجسس أو الانتحال.

هذا الاطمئنان مفهوم، لكنه ليس أبديًا. فالتاريخ التقني يبيّن أن أدوات الحماية لا تبقى صالحة بالدرجة نفسها إلى ما لا نهاية. بعض الخوارزميات كانت قوية في زمنها ثم تراجعت قيمتها مع تطور القدرة الحسابية وظهور طرق تحليل جديدة. واليوم يبرز نقاش جدّي حول أثر الحوسبة الكوانتية في مستقبل الأمن الرقمي، ليس لأن هذا الخطر تحقق عمليًا على نطاق واسع، بل لأن تجاهله حتى اللحظة الأخيرة سيكون خطأً استراتيجيًا.

هنا يظهر مفهوم التشفير ما بعد الكوانتم بوصفه استجابة علمية وعملية لهذا التحول المحتمل. والمقصود به خوارزميات تشفير جديدة صُممت لتبقى مقاومة للهجمات حتى في حال توفر حواسيب كوانتية قوية في المستقبل. ولا تكمن أهمية هذا التوجه في بعده النظري فقط، بل في كونه تحولًا بدأ يدخل فعليًا إلى مسار المعايير الدولية والتخطيط المؤسسي. ومن ثم فإن السؤال لم يعد: هل يستحق الأمر التفكير؟ بل أصبح: كيف يمكن الاستعداد المبكر بطريقة علمية متوازنة، بعيدة عن التهويل وبعيدة كذلك عن اللامبالاة؟

2. ما الذي قد يتغير مع الحوسبة الكوانتية؟

الحوسبة الكوانتية ليست مجرد نسخة أسرع من الحواسيب التقليدية، بل هي نمط مختلف من المعالجة يعتمد على مبادئ فيزيائية مغايرة لما نعرفه في الحوسبة الكلاسيكية. وهذا لا يعني أن كل ما هو رقمي اليوم سينهار غدًا، ولا يعني أيضًا أن الحاسوب الكوانتي سيجعل كل وسائل الأمن بلا قيمة. لكن بعض أنظمة الحماية المعتمدة حاليًا، ولا سيما في التشفير بالمفتاح العام، ترتكز على مسائل رياضية يُعتقد أن الحوسبة الكوانتية قد تجعل حلّها أسهل بكثير مما هو عليه اليوم.

ومن المهم هنا التمييز بين نوعين من التشفير يختلطان في النقاش العام. هناك أولًا ما يسمى التشفير الكمي، وهو مجال مختلف يرتبط بوسائط اتصال وتقنيات فيزيائية خاصة. وهناك ثانيًا التشفير ما بعد الكوانتم، وهو المقصود في هذا المقال، ويعني خوارزميات جديدة يمكن تشغيلها على البنى الرقمية المعتادة، لكنها مصممة كي تتحمل خصمًا قد يمتلك قدرات كوانتية في المستقبل. هذا التمييز ليس لغويًا فقط؛ فالخلط بين المصطلحين يفسد الفهم العلمي للموضوع منذ البداية.

كما ينبغي تجنب المبالغة. فليس صحيحًا أن جميع أشكال التشفير الحالي ستسقط دفعة واحدة. الخطر يتركز بدرجة أكبر على بعض الآليات المستخدمة في تبادل المفاتيح والتوقيع الرقمي، أي في تلك الأجزاء التي تُشكل أساس الثقة في الاتصالات والهوية الرقمية. ولذلك فإن القضية المطروحة اليوم ليست إعلان موت الأمن الرقمي، بل إعادة بناء بعض أعمدته الأساسية قبل أن يصبح التأخر مكلفًا.

3. ما المقصود بالتشفير ما بعد الكوانتم؟

يمكن تبسيط الفكرة بالقول إن التشفير ما بعد الكوانتم هو جيل جديد من الخوارزميات بُني على مسائل رياضية مختلفة عن تلك التي اعتمدت عليها كثير من الأنظمة المشهورة خلال العقود الماضية. الغاية من هذا الجيل الجديد هي توفير بدائل أكثر صمودًا في وجه الهجمات المتوقعة من خصم يملك في المستقبل حاسوبًا كوانتيًا ذا أثر عملي في كسر بعض الأنظمة الحالية.

وتكتسب هذه الفكرة أهميتها من أن العالم لم يعد يتعامل معها باعتبارها فرضية بعيدة. فقد دخلت إلى قلب النقاش المعياري العالمي، وبدأت مؤسسات مرجعية في الأمن السيبراني بدفع المنظمات إلى الاستعداد للانتقال إليها. هذا يعني أن الموضوع انتقل من مرحلة الفضول العلمي إلى مرحلة التخطيط والتجريب والتهيئة المؤسسية.

لكن قوة الفكرة لا تعني أن الطريق سهل. فالخوارزميات الجديدة لا تكون دائمًا بديلًا مباشرًا يمكن إدخاله في الأنظمة القديمة بضغطة زر. بعضها يحتاج إلى تعديلات في البرمجيات والبروتوكولات، وبعضها يفرض أحجامًا مختلفة للمفاتيح أو للتواقيع أو للأداء. لهذا السبب فإن الحديث عن التشفير ما بعد الكوانتم ليس حديثًا عن خوارزمية جديدة فقط، بل عن عملية انتقال واسعة تمس المنتجات والخدمات والبنية التحتية والحوكمة الرقمية في آن واحد.

4. لماذا يجب الاستعداد الآن لا لاحقًا؟

قد يعترض البعض قائلاً إن الحاسوب الكوانتي القادر فعلًا على إحداث هذا التحول لم يصبح بعد جزءًا من الواقع العملي العام، فلماذا كل هذا الاهتمام؟ والجواب أن الأمن الرقمي لا يُدار بردود الفعل المتأخرة، بل بالتوقع والاستباق. فالانتقال من خوارزميات مستقرة استُخدمت لسنوات طويلة إلى خوارزميات جديدة يحتاج إلى وقت كبير، ويشمل الجرد، والاختبار، والتوافق، والتحديث، والتدريب، والتكلفة، وإدارة المخاطر. ومن يعتقد أن الانتقال يمكن أن يبدأ عند وقوع الخطر يكون في الحقيقة قد قرر أن يبدأ متأخرًا.

هناك سبب آخر أكثر حساسية، وهو ما يعرف في الأدبيات الحديثة بفكرة «احصد الآن وفكّ التشفير لاحقًا». ومعناها أن جهة معادية قد لا تكون قادرة اليوم على قراءة البيانات المحمية، لكنها تستطيع جمعها وتخزينها أملًا في فكها مستقبلًا إذا توفرت قدرات كوانتية كافية. وهذا يجعل المسألة غير مرتبطة فقط بحاضر الأمن، بل بعمر البيانات نفسها. فالبيانات التي تبقى حساسة لسنوات طويلة، مثل الوثائق الحكومية الحساسة أو الملكية الفكرية أو بعض البيانات الطبية أو الصناعية، قد تصبح هدفًا لهذا النوع من التفكير بعيد المدى.

ومن هنا فإن الاستعداد المبكر لا يُفهم بوصفه ذعرًا تقنيًا، بل بوصفه سياسة عقلانية لحماية البيانات ذات القيمة الزمنية الطويلة. إن أخطر ما في التحولات التكنولوجية الكبرى ليس أنها تأتي فجأة، بل أن المؤسسات كثيرًا ما ترى إشاراتها مبكرًا ثم تؤجل الاستجابة حتى يصبح التغيير أعقد وأكثر كلفة.

5. التحدي الحقيقي ليس الاختراع بل الهجرة

في الخطاب الإعلامي السطحي يبدو الأمر أحيانًا وكأنه مجرد إعلان عن خوارزميات جديدة، ثم ينتهي النقاش. لكن الحقيقة أن أصعب جزء في هذا الملف ليس إنتاج الخوارزمية نفسها، بل نقل الأنظمة إليها بطريقة منظمة وآمنة. فالمؤسسة

الحديثة لا تعتمد على خدمة واحدة أو جهاز واحد، بل على منظومة مترابطة من البرمجيات، وقواعد البيانات، والشهادات الرقمية، وأجهزة الشبكات، والخدمات السحابية، والتطبيقات القديمة، وأنظمة المورّدين الخارجيين. وكل عنصر من هذه العناصر قد يتضمن اعتمادًا صريحًا أو خفيًا على بنى تشفير معينة.

لهذا السبب يبرز مفهوم الجرد التشفيري بوصفه نقطة البداية المنطقية. فلا يمكن الانتقال إلى ما بعد الكوانتم إذا كانت المؤسسة لا تعرف أصلًا أين تستخدم التشفير، وبأي خوارزميات، وفي أيّ تطبيقات، وتحت أيّ تبعيات تقنية. وبعد الجرد تأتي مسألة الأولويات: ما الأنظمة الأكثر حساسية؟ ما الخدمات التي تتعامل مع بيانات تبقى قيمتها عالية لسنوات؟ ما التطبيقات التي سيكون تحديثها سهلًا؟ وأيها يتطلب إعادة تصميم أو تغييرًا في البنية؟

كما أن الهجرة لا تتعلق فقط بالجانب البرمجي، بل بالعامل البشري والحوكمي أيضًا. فالفِرق التقنية تحتاج إلى تكوين، وإدارات المخاطر تحتاج إلى فهم جديد، وصنّاع القرار يحتاجون إلى رؤية زمنية وتمويلية، والمورّدون مطالبون بإعلان جاهزيتهم وخططهم. لهذا يبدو الانتقال إلى التشفير ما بعد الكوانتم أقرب إلى مشروع تحوّل مؤسسي متعدد الطبقات منه إلى تحديث تقني محدود.

مسار الانتقال من الأنظمة الحالية إلى الهجرة التدريجية نحو التشفير ما بعد الكوانتم

6. بين الأمل والواقع: كيف نقرأ المسار الحالي؟

من الخطأ التعامل مع التشفير ما بعد الكوانتم وكأنه حل سحري أُنجز بالكامل، كما أنه من الخطأ المقابل اعتباره فكرة بعيدة لا تستحق الجهد. القراءة العلمية الرصينة تقتضي موقفًا وسطًا: هناك تقدّم حقيقي في المعايير وفي الاختيار العلمي للخوارزميات، وهناك أيضًا تحديات عملية تتعلق بالأداء والتوافق والانتشار والاختبار طويل المدى. وهذا طبيعي في أيّ تحول تقني جذري.

إن نضج المعايير الدولية يعطي إشارة مهمة مفادها أن العالم بدأ يخرج من مرحلة الانتظار النظري. لكن هذا لا يلغي الحاجة إلى الحذر في التطبيق. فالأنظمة الحساسة لا تُحدَّث على أساس الحماسة، بل على أساس الاختبار والتدرج والتحقق من الأثر على الواقع التشغيلي. ومن هنا تبرز قيمة الحلول الانتقالية التي تجمع بين المحافظة على الاستقرار الحالي والتهيئة للمرحلة المقبلة، بدل القفز غير المحسوب أو الجمود غير المبرر.

والأهم من ذلك أن هذا المسار يذكّرنا بأن الأمن الرقمي ليس منتجًا نهائيًا نشتريه مرة واحدة، بل قدرة مؤسسية على التكيف المستمر. والمؤسسات التي تفهم هذه الحقيقة مبكرًا ستكون أقدر على تحويل التحدي إلى فرصة لبناء بنية رقمية أكثر نضجًا ومرونة.

7. ماذا يعني هذا للعالم العربي والجامعة والمؤسسة؟

قد يظن بعض القراء أن هذا النقاش يخص الشركات الكبرى أو الدول الصناعية وحدها، وأنه ما يزال بعيدًا عن الجامعات والمؤسسات العربية، غير أن هذا التصور يحتاج إلى مراجعة. فمعظم المؤسسات العربية تعتمد اليوم على نظم تشغيل عالمية، وخدمات سحابية، ومنتجات أمنية، وشهادات رقمية، وبروتوكولات اتصال دولية. وعندما يتغير معيار الحماية في العالم، فإن أثر ذلك لا يبقى محصورًا في بلد دون آخر.

بالنسبة إلى الجامعات، يطرح الموضوع بعدين مهمين. البعد الأول معرفي وتكويني، لأن تكوين الطلبة في الإعلام الآلي والهندسة والأمن السيبراني لا ينبغي أن يظل أسير الأدوات القديمة فقط، بل يجب أن يفتح النقاش حول التحولات القادمة في التشفير والمعايير والبروتوكولات. والبعد الثاني مؤسسي، لأن الجامعات نفسها تدير منصات تعليمية، وأرشيفات رقمية، وبريدًا إلكترونيًا، وخدمات مصادقة، ووثائق إدارية، وكلها تحتاج مع الوقت إلى رؤية أوضح بشأن التحول التشفيري.

أما في المؤسسات العامة والخاصة، فإن الحد الأدنى العقلاني لا يبدأ بشراء حلول غامضة تحت شعارات كوانتية براقة، بل يبدأ بأسئلة بسيطة: ما الأصول الرقمية التي نملكها؟ ما عمر الحساسية المتوقع لبياناتنا؟ ما المورّدون الذين سنعتمد عليهم في هذا التحول؟ وهل لدينا خريطة واضحة لاعتماداتنا التشفيرية؟ إن أول خطوة ناضجة ليست تقنية بحتة، بل إدارية معرفية: أن نعرف ماذا لدينا قبل أن نقرر إلى أين نذهب.

8. خاتمة

إن التشفير ما بعد الكوانتم ليس عنوانًا دعائيًا لموجة تقنية جديدة، بل هو تعبير عن تحوّل عميق في طريقة التفكير في أمن البيانات على المدى الطويل. فالقضية لا تتعلق بالخوف من آلة لم تنضج بعد، وإنما بفهم أن بعض البنى التي نثق بها اليوم قد لا تحتفظ بالصلابة نفسها في المستقبل. وبين المبالغة التي تزعم انهيارًا وشيكًا لكل شيء، والتراخي الذي يرفض الاستعداد بحجة أن الخطر لم يقع بعد، يظل الموقف العلمي الرشيد هو الاستعداد المبكر والمتدرج.

لقد أثبت التاريخ أن تكلفة التحديث الوقائي أقل بكثير من تكلفة التدارك المتأخر، خاصة حين يتعلق الأمر ببنى رقمية واسعة ومعقدة. ولذلك فإن أفضل ما يمكن للمؤسسات والجامعات والهيئات التنظيمية فعله اليوم ليس انتظار اليقين الكامل، بل بناء وعي مؤسسي، والبدء في الجرد، ومتابعة المعايير، وتكوين الكفاءات، والتخطيط لهجرة تدريجية ومسؤولة.

وبهذا المعنى، فإن الاستعداد لما بعد الكوانتم ليس انشغالًا بالمستقبل البعيد بقدر ما هو دفاع ذكي عن الحاضر نفسه؛ لأن البيانات التي نريد حمايتها غدًا قد تكون هي البيانات التي تُجمَع اليوم.

المراجع

[1] National Institute of Standards and Technology (NIST), *NIST Releases First 3 Finalized Post-Quantum Encryption Standards*, 2024.

[2] NIST, *What is Post-Quantum Cryptography?*, 2024.

[3] NIST Computer Security Resource Center (CSRC), *Post-Quantum Cryptography*, updated 2025.

[4] NIST National Cybersecurity Center of Excellence (NCCoE), *Migration to Post-Quantum Cryptography*, 2025.

[5] National Cyber Security Centre (NCSC), *Timelines for Migration to Post-Quantum Cryptography*, 2025.