تظهر الأبحاث أن مستقبل التشفير يتأثر بشكل كبير بالتطورات في التشفير الكمومي والتشفير المنحني الإهليلجي. تتميز تقنية توزيع المفاتيح الكمومية (QKD) بأمانها الاستثنائي، باستخدام مبادئ ميكانيكا الكم لجعل التنصت قابلاً للكشف. وهذا يجعل توزيع المفاتيح الكمومية RSA دفاعًا واعدًا ضد التهديدات التي تشكلها الحوسبة الكمومية، والتي يمكن أن تعرض الأنظمة التقليدية مثل شائعة بسبب كفاءتها وأمانها القوي مع أحجام مفاتيح (ECC) للخطر. بالإضافة إلى ذلك، أصبحت تقنية تشفير المنحنى الإهليلجي ليست محصنة ضد الهجمات ECC أصغر، مما يجعلها مثالية للأجهزة المحمولة وأجهزة إنترنت الأشياء. من المهم ملاحظة أن الكمومية، مما يسلط الضوء على الحاجة إلى الانتقال إلى خوارزميات مقاومة للكم. يتم تشجيع المنظمات على تبني هذه الأساليب التشفيرية في المستقبل لعدة أسباب. فهي توفر أداءً محسنًا لتشفير المفتاح العام بأحجام مفاتيح أقصر، وهو مناسب بشكل خاص للأجهزة المحمولة وأجهزة إنترنت الأشياء. يتعين على المنظمات الاستثمار في أنظمة هجينة تستخدم خوارزميات كلاسيكية ومقاومة للكميات، إلى جانب البحث والتطوير، والالتزام بمعايير الصناعة، ومن شأن هذا النهج أن يعزز حماية البيانات، ويجهزها لمواجهة التهديدات السيبرانية المعقدة.