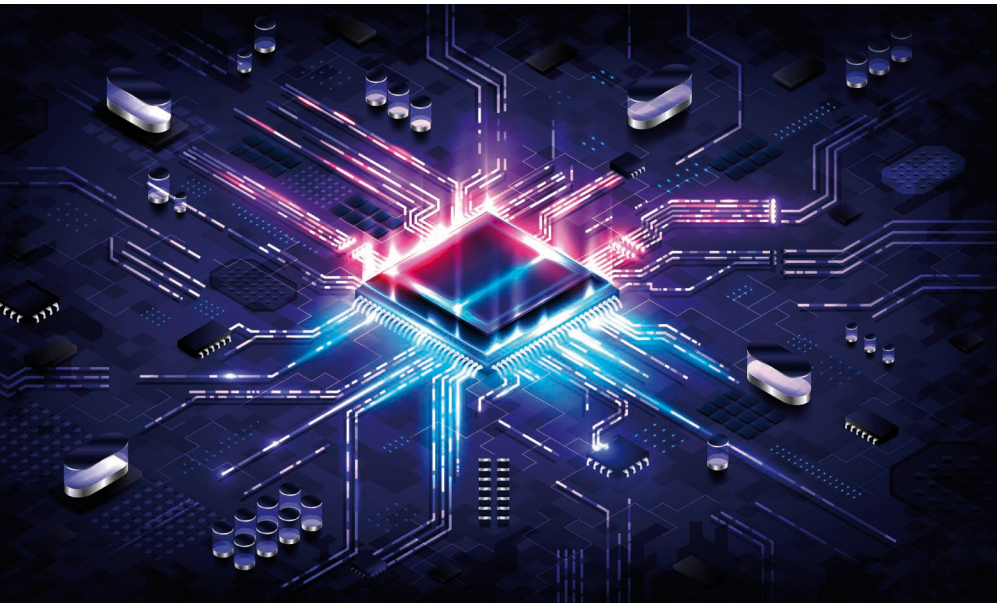
Cybersicherheit im Quantenzeitalter

Wie Daten schon heute für morgen sicher gemacht werden



Symbolische Darstellung eines Quantencomputers – die Bedrohung für klassische Verschlüsselung

Von der Vorsorge zur digitalen Verteidigung: Quantencomputer stellen die bisherige Verschlüsselung auf den Prüfstand – und damit unsere digitale Sicherheit. Warum Europol zur Eile mahnt, welche Rolle deutsche Halbleiterhersteller spielen und was Ihre Daten mit der Weisheit meiner Großmutter zu tun haben.

Die reale Bedrohung

Crash-Propheten hatten noch nie Sendepause. Doch wenn selbst meine konservative Großmutter, Kind der Nachkriegszeit, mir mitgab: „Spare, wenn du hast, dann hast du in der Not“, dann klingt das heute wie ein Appell zur digitalen Vorsorge. Denn der Verteidigungsfall kommt nicht als Angriff mit Panzern, sondern als Angriff auf unsere Daten. Die Bedrohung ist real: Europol warnt vor organisierten Netzwerken, die bereits heute verschlüsselte Daten sammeln, um sie später mit Quantencomputern zu entschlüsseln und somit für sich nutzbar zu machen [1]. Das Szenario nennt sich „store now, decrypt later“.

Quantencomputer sind dabei, die Spielregeln der Kryptografie grundlegend zu verändern. Algorithmen wie RSA (Rivest-Shamir-Adleman), auf denen ein Großteil unserer digitalen Kommunikation basiert, könnten schon bald von Quantencomputern geknackt werden. Post-Quantum-Kryptografie (PQC) heißt die Antwort darauf: Also neue kryptografische Verfahren, die auch im Zeitalter der Quantenrechner Bestand haben.

Es ist Zeit zu handeln

Quantenbedrohung rückt näher: Die Fortschritte im Quantencomputing sind rasant. Große Tech-Konzerne, Universitäten und Start-ups überbieten sich mit Erfolgsmeldungen. Gleichzeitig reagiert die Sicherheitsforschung: Das US-amerikanische National Institute of Standards and Technology (NIST) hat bereits drei Algorithmen als Post-Quantum-Standards definiert: Die Federal Information Processing Standards (FIPS) FIPS-203 (ML-KEM), 204 und 205 bieten robuste Mechanismen für Schlüsselaustausch und digitale Signaturen, die Angriffen von Quantencomputern standhalten.

Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat seine Einschätzung zum so genannten „Q-Day“ abgegeben – dem Tag, an dem Quantencomputer erstmals in der Lage sein werden, herkömmliche Verschlüsselung praktisch zu brechen. Das BSI rechnet bereits um das Jahr 2030 damit – also etwa zu dem Zeitpunkt, an dem heutige Elektronikentwicklungen in Serie gehen. Wer sich also jetzt nicht vorbereitet, läuft Gefahr, später mit veralteter Sicherheitstechnik zu produzieren.

Und auch das von Europol initiierte Quantum Safe Financial Forum (QSFF) drängt darauf, insbesondere den Finanzsektor schon jetzt mit den heute verfügbaren Mitteln gegen die morgen verfügbare Technik abzusichern.

Herausforderungen

bei der Umstellung auf Post-Quanten-Kryptografie: So klar das Ziel ist, so anspruchsvoll ist der Weg dorthin. Größere Schlüssel und komplexere Algorithmen erfordern mehr Rechenleistung – eine Herausforderung besonders für ältere Systeme. Zudem ist die Standardisierung noch nicht vollständig abgeschlossen, sodass sich die verwendeten Algorithmen in Zukunft noch ändern können. Und auch organisatorisch ist der Umstieg kein Selbstläufer – er erfordert Investitionen, Umdenken und technisches Know-how. Der Schlüssel zum Erfolg liegt daher in der sogenannten Kryptoagilität: Systeme sollten von Anfang an so flexibel gestaltet werden, dass sie schnell auf neue Erkenntnisse oder Bedrohungen reagieren können.

Erste Schritte

zu einer sicheren IT-Infrastruktur im Quantenzeitalter: Trotz dieser Herausforderungen zeigen erste praktische Umsetzungen, dass der Wandel zur Post-Quanten-Kryptografie bereits begonnen hat: Infineon, Rutroniks größter Franchisepartner, hat sich frühzeitig als Vorreiter in Sachen PQC positioniert. Bereits 2017 wurde ein quantenresistenter Schlüsselaustausch auf einem kontaktlosen Chip umgesetzt [2].

Exkurs: Zufall ist nicht gleich Zufall

TRNG, PRNG, QRNG – hinter diesen Kürzeln verbergen sich unterschiedliche Verfahren zur Generierung kryptografisch notwendiger Zufallszahlen.
PRNGs (Pseudo Random Number Generators) erzeugen Zahlen durch deterministische Prozesse, die mit genügend Wissen reproduzierbar sind. TRNGs (True Random Number Generators) nutzen physikalische Prozesse, sind aber nicht vollständig manipulationssicher. Erst QRNGs (Quantum Random Number Generators) liefern wirklich nicht vorhersagbare Zufallszahlen, da sie auf quantenphysikalischen Effekten wie der Emission einzelner Photonen basieren – ein elementarer Sicherheitsvorteil für die Kryptografie von morgen.

Autor:
Bernd Hantsche
Vice President
Technology Competence Center
Rutronik
www.rutronik.com

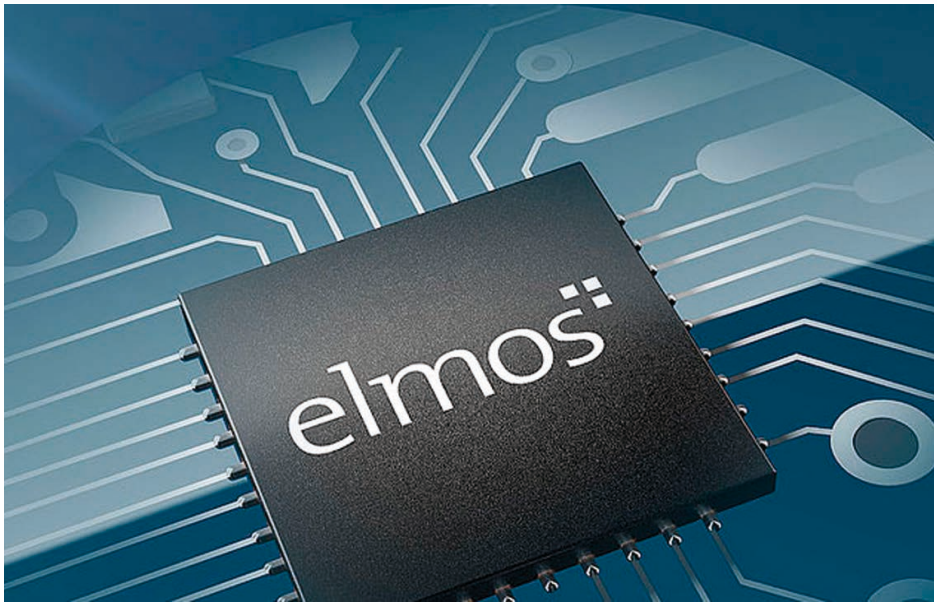


Bild 1: Miniaturisierter QRNG-Baustein von Elmos Semiconductor – echte Zufälligkeit für vernetzte Geräte der nächsten Generation

Anfang 2025 folgte die weltweit erste EAL6-Zertifizierung durch das BSI für einen Sicherheitscontroller mit ML-KEM-Verfahren [3]. Damit deckt Infineon insbesondere Smartcard-Anwendungen ab.

Auch andere deutsche Halbleiterhersteller treiben die Entwicklung voran. Elmos Semiconductor legt nun, gemeinsam mit ID Quantique, mit einem für das PQC wichtigen Baustein nach, einem miniaturisierten Quantum Random Number Generator (QRNG).

Verschlüsselungsverfahren

Jedes Verschlüsselungsverfahren beginnt mit einer Zufallszahl für die Schlüsselerzeugung. Die Erzeugung einer solche Zufallszahl ist für einen logisch und diskret arbeitenden Apparat jedoch eine große Herausforderung. HRNG, Hardware Random Number Generator, gibt es seit langem und in verschiedenen technischen Ausführungen. Herkömmliche Generatoren (TRNG/PRNG) sind manipulierbar – durch physikalische Einflüsse, wie Licht, Druck, Temperatur, elektromagnetische Felder und Versorgungsspannung oder durch gezielte Eingriffe durch Künstliche Intelligenz.

QRNG nutzt echte Quanteneffekte wie die Emission von Photonen, um wirklich zufällige Zahlen zu generieren. Das ist nicht nur sicherer, sondern auch eine zwingende Voraussetzung für FIPS-203/204/205-konforme Kryptografie. Solche QRND-Lösungen sind bisher eher als Erweiterungssteckkarten für Server bekannt. Elmos hat die Technologie nun miniaturisiert und in ein 2x2 mm DFN-Gehäuse gepackt (Bild 1). Damit steht die patentierte Technologie über Rutronik allen Kunden weltweit zur Verfügung. Neben der Finanzbranche profitieren auch die Bereiche Industrie, Medizin und Automotive.

Sicherheit ist kein Luxus, sondern Pflicht

Denn: Es geht längst nicht mehr nur um Banken. Ob Industrieanlagen, medizinische Geräte oder Fahrzeuge mit Assistenzsystemen – unsere Welt ist digital, vernetzt und damit angreifbar. Was passiert, wenn die Assistenzsysteme in Fahrzeugen plötzlich Verkehrsschilder falsch erkennen, wenn sich Fahrzeuge per Ultra-Wideband-Technologie und Rolling-Key-Verfahren öffnen lassen, weil der Schlüssel vorhersehbar war? Oder wenn medizinische Daten abgefangen werden, weil der Zufallszahlengenerator nicht echt war?

Die Quantenrevolution kommt.

Vielleicht nicht morgen, aber sicher – früher als viele hoffen. Wer heute nicht investiert, wird morgen zahlen. Um es mit der Weisheit meiner inzwischen verstorbenen Großmutter zu sagen: „Verschlüssele deine Daten heute vernünftig, dann bist du auch morgen vor Quanten-Cyberangriffen geschützt."

Quellen:

[1] www.europol.europa.eu/media-press/newsroom/news/call-for-action-urgent-plan-needed-to-transition-to-post-quantum-cryptography-together

[2] www.infineon.com/cms/en/product/promopages/post-quantum-cryptography/

[3] www.infineon.com/cms/de/about-infineon/press/press-releases/2025/INFCSS202501-043.html#_ftnref1

Begriffe auf einen Blick:

- **Q-Day –** Der Zeitpunkt, an dem Quantencomputer in der Lage sein werden, heutige Verschlüsselungssysteme zu brechen. Das BSI erwartet ihn etwa 2030.
- **QRNG vs. TRNG –** Quantum Random Number Generators erzeugen echte, nicht manipulierbare Zufallszahlen auf Basis quantenphysikalischer Prozesse. TRNGs nutzen physikalische Effekte, sind aber potenziell störanfällig.
- **FIPS-203/204/205 –** Vom NIST veröffentlichte Sicherheitsstandards für quantensichere Algorithmen (Schlüsselaustausch und digitale Signaturen), als Basis für Post-Quantum-Kryptografie.
- **ML-KEM** (Module Lattice Key Encapsulation Mechanism) ist ein Schlüsselkapselungsmechanismus (KEM), der von NIST als FIPS 203 standardisiert wurde. Er dient dazu, einen sicheren, gemeinsamen Geheimnisschlüssel zwischen zwei Parteien zu etablieren, der gegen klassische und Quantencomputerangriffe resistent ist. ◄