ISSN: 2585-2388

ΣΕΠΤΕΜΒΡΙΟΣ 2026, ΤΙΜΗ 9,00 ΕΥΡΩ, ΤΕΥΧΟΣ No.503

netweek

Leading the Digital Business Revolution!

SPECIAL REPORTS

Quantum Computing: Ανοίγοντας τον δοκιμαστικό σωλήνα

Data Management & Analytics: Καταλύτης για ορθότερες αποφάσεις

Health IT: Υγεία να 'χουμε... και AI προλαμβάνειν

ENTERPRISE SERVICE MANAGEMENT:

Η αθέατη προϋπόθεση του σύγχρονου ψηφιακού μετασχηματισμού

COSMOS BUSINESS SYSTEMS

RRF: Από ανάδοχος σε στρατηγικό συνεργάτη

Δημήτρης Δάφνης, Πρόεδρος & Διευθύνων Σύμβουλος

Ανοίγοντας τον δοκιμαστικό σωλήνα

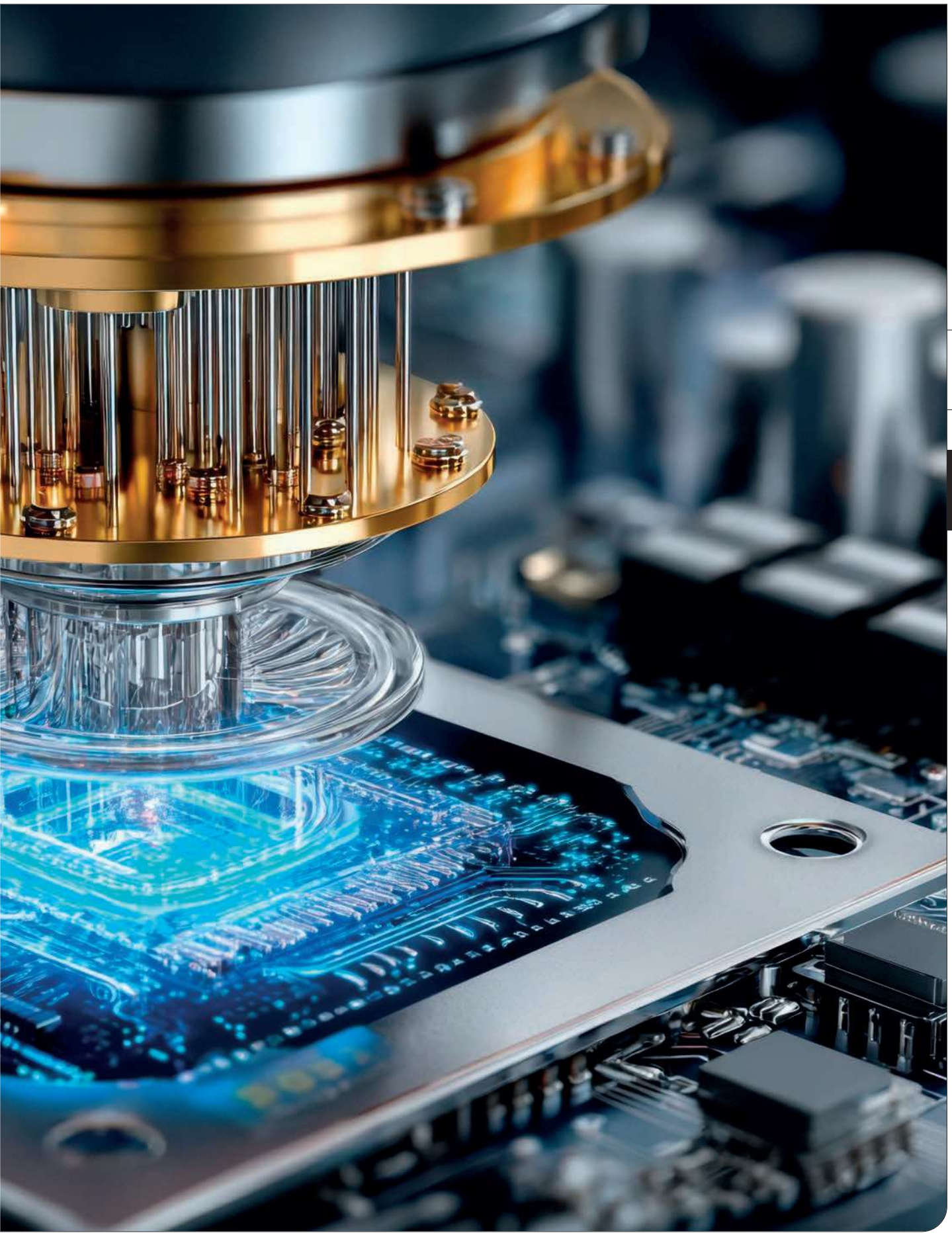
Το quantum computing συνεχίζει να εξελίσσεται και να εντυπωσιάζει ως «η άλλη τρομερή αναδυόμενη τεχνολογία», αλλά και σταδιακά να περνάει από τη φάση της θεωρητικής «υπόθεσης εργασίας» σε αυτή του να απαντήσει σε ερωτήσεις για το μέλλον του.

ΤΟΥ ΒΑΓΓΕΛΗ ΒΑΓΓΕΛΑΤΟΥ

Το quantum computing περνά μια μεταβατική περίοδο. Για παραπάνω από μία δεκαετία ήταν μια τεχνολογία συνδεδεμένη κυρίως με εργαστηριακά και άκρως πειραματικά περιβάλλοντα. Μια περιπέτεια δημιουργίας και διαχείρισης qubits και θεωρητικές προσεγγίσεις μιας «άλλης» θαυματουργής όσο και ακατανόητης για τους περισσότερους δυνατότητας «υπερ-υπολογισμού». Φλερτάροντας εξίσου με τα ανώτερα μαθηματικά και την κβαντική φυσική, όσο και μηχανικές προκλήσεις -κυρίως στο ζήτημα της υπερψύξης των συστημάτων- διατηρούσε τη «μαγική» του διάσταση, ανάλογη με εκείνη κάθε πραγματικά ριζοσπαστικής τεχνολογικής εξέλιξης.

Σταδιακά όμως η quantum computing ατζέντα αλλάζει: επιχειρήσεις τεστάρουν κβαντικούς αλγόριθμους και προσπαθούν να προβλέψουν πότε η κβαντική υπολογιστική θα εξαπλωθεί και σε ποιους τομείς, ώστε να την εντάξουν στα στρατηγικά τους σχέδια. Tech κολοσσοί επενδύουν σε quantum υποδομές. Και κυβερνήσεις και οργανισμοί προσπαθούν να ετοιμαστούν για την ώρα που κάθε ψηφιακή κρυπτογράφηση θα είναι εν δυνάμει υποψήφιο θύμα ενός κβαντικού υπερ-υπολογιστή.

Έτσι το πεδίο του κβαντικού ανταγωνισμού έχει τόσο μεγάλα ονόματα όσο και εξειδικευμένους παίκτες. Οι IBM, Google Quantum AI, Microsoft Quantum και η Amazon Web Services, ορίζουν με το βάρος τους το γήπεδο του εμπορικού ανταγωνισμού, αλλά και με διαφορετικές στρατηγικές. Η IBM εστιάζει σε συστήματα υπερυπολογιστών τα οποία προσφέρουν εμπορική πρόσβαση. Η Google στη διόρθωση λάθους. Η Microsoft στην τοπολογία των qubits και στη δημιουργία μιας πιο ανθεκτικής στα λάθη αρχιτεκτονικής. Και η AWS στην παροχή μέσω cloud πρόσβασης σε τεχνολογίες quantum computing μέσω της πλατφόρμας της Braket. Την ίδια στιγμή μικρότεροι αλλά εξειδικευμένοι παίκτες είναι εξίσου σημαντικοί για τις εξελίξεις.



Οι Quantinuum, IonQ, Rigetti Computing, D-Wave και Pasqal, αντιπροσωπεύουν διαφορετικές προσεγγίσεις οι οποίες συμπεριλαμβάνουν τεχνολογίες παγιδευμένων ιόντων (trapped ion, χρήση μεμονωμένων φορτισμένων ατόμων που ακινητοποιούνται σε κενό μέσω ηλεκτρομαγνητικών πεδίων), τεχνολογίες υπεραγωγιμότητας (superconducting, χρήση μικροσκοπικών υπεραγώγιμων κυκλωμάτων qubits που λειτουργούν σε θερμοκρασίες κοντά στο απόλυτο μηδέν), τεχνολογίες «κβαντικής ανόπτησης» (annealing) και τεχνολογίες ουδέτερων ατόμων (neutral atom tech, χρήση ηλεκτρικά ουδέτερων ατόμων τα οποία παγιδεύονται και μετακινούνται με τη βοήθεια εστιασμένων δεσμών λέιζερ).

Και αυτό είναι ένα ακόμα πρόβλημα για τον επιχειρηματικό κόσμο, ο οποίος πέρα από τη δυσκολία του να καταλάβει την ίδια την αρχή λειτουργίας της κβαντικής υπολογιστικής, δυσκολεύεται να δει πού πρέπει να επενδύσει, πριν όλες αυτές οι τεχνολογίες αποκρυσταλλωθούν σε ένα επικρατέστερο μοντέλο λειτουργίας.

Η μεταβατική περίοδος για τη νέα τεχνολογία ορίζεται από δύο γεγονότα: από τη μία ότι ως τεχνολογία είναι ακόμα αρκετά μακριά από το να είναι έτοιμη για πραγματικά ευρεία εμπορική εξάπλωση. Και από την άλλη ότι οι άνθρωποι του οικοσυστήματός της ξεκίνησαν ήδη να απαντούν στις βασικές δημοσιογραφικές ερωτήσεις, «ποιος-πού-πώς-πότε-γιατί» για τη χρήση της στον πραγματικό κόσμο.

Το quantum computing βγαίνει σταδιακά από το εργαστήριο, αναζητώντας τις εφαρμογές που θα αποδείξουν την πραγματική επιχειρηματική του αξία

Από τη θεωρία στην πράξη

Και για να ανακαλύψουμε πόσο κοντά βρίσκεται στην ελληνική πραγματικότητα, το netweek έθεσε τα βασικά αυτά ερωτήματα στον Ηλία Κ. Σάββα, καθηγητή του Τμήματος Ψηφιακών Συστημάτων, στο Πανεπιστήμιο Θεσσαλίας, με ερευνητικά ενδιαφέροντα την κβαντική υπολογιστική, τα παράλληλα και κατανεμημένα συστήματα, τα υπολογιστικά νέφη και τα συστήματα υψηλών επιδόσεων. Με πρώτο το ερώτημα αν όντως η κβαντική υπολογιστική περνάει από τη θεωρία στην πράξη.

«Η κβαντική υπολογιστική περνά σταδιακά από το εργαστήριο και τη θεωρητική έρευνα σε μια νέα φάση, όπου οι πρώτες πραγματικές εφαρμογές αρχίζουν να διερευνώνται» μας εξηγεί. «Δεν βρισκόμαστε ακόμη στην εποχή των “κβαντικών υπολογιστών για όλους”, όμως βρισκόμαστε ήδη σε ένα σημείο όπου η τεχνολογία αυτή διαμορφώνει το επόμενο κεφάλαιο της πληροφορικής».

Η έρευνα της McKinsey «Quantum Technology Monitor 2025: The Year of Quantum: From Concept to Reality in 2025» περιγράφει και αυτή ακριβώς αυτό. Μια περίοδο όπου οι υπάρχοντες κβαντικοί υπολογιστές παλεύουν με τα όρια τους, κυρίως σε ό,τι αφορά τη διαχείριση του προβλήματος του «θορύβου» και των λαθών που προκαλεί και πολλές πρακτικές εφαρμογές είναι ακόμα είτε πειραματικές είτε ενσωματώνουν ένα υβριδικό μοντέλο όπου η «συμβατική» υπολογιστική συνδυάζεται με την κβαντική για να δώσει αξιόπιστα και εύχρηστα αποτελέσματα. Παρ’ όλες τις δυσκολίες όμως η ίδια έρευνα καταγράφει μια τεράστια δυναμική, με τη δημιουργία αξίας να εκτιμάται στα 97 δισεκατομμύρια δολάρια ανά έτος ως το 2035.

Δυναμικότερες προοπτικές μάλιστα αναφέρει τη χρήση της κβαντικής υπολογιστικής στην κρυπτογράφηση της μετάδοσης δεδομένων -όπως ήταν αναμενόμενο- και στη μέτρηση με εξωπραγματική ακρίβεια διαστάσεων στον φυσικό κόσμο. Όπως μας λέει και ο Ηλίας Σάββας «από την ελληνική ερευνητική σκοπιά, ιδιαίτερο ενδιαφέρον παρουσιάζουν πεδία στα οποία η κβαντική υπολογιστική θα μπορούσε να προσφέρει νέες προσεγγίσεις σε δύσκολα υπολογιστικά προβλήματα. Μεταξύ αυτών βρίσκονται η βελτιστοποίηση σύνθετων συστημάτων και δικτύων, η προσομοίωση μοριακών και υλικών δομών, η κρυπτογραφία και η κυβερνοασφάλεια, αλλά και η μηχανική μάθηση. Παράλληλα, η Ελλάδα διαθέτει ένα ολοένα πιο ενεργό οικοσύστημα ερευνητών και εκπαιδευτικών πρωτοβουλιών, γεγονός ιδιαίτερα σημαντικό, καθώς η κβαντική τεχνολογία δεν είναι μόνο ζήτημα υποδομών αλλά είναι, πάνω απ’ όλα, ζήτημα ανθρώπινου δυναμικού και γνώσης».

Οικονομία - Μικρόκοσμος - Βιομηχανία - Ασφάλεια

Με έναν εξίσου θαυμαστό τρόπο η κβαντική υπολογιστική φαίνεται ότι θα γεφυρώσει πρώτα αυτά τα τέσσερα σύμπαντα, αφού εκεί είναι ήδη τα πρώτα πεδία δοκιμαστικής εφαρμογής.

Όπως σημειώνει όμως και η έκθεση «Quantum Computing Guide for Business Leaders», της Deloitte, η κβαντική υπολογιστική δεν μπορεί να θεωρηθεί ως μια άμεση διάδοχη κατάσταση των παραδοσιακών υπολογιστικών συστημάτων. Αλλά ως ένα εξειδικευμένο εργαλείο για μια συγκεκριμένη «κλάση» προβλημάτων. Ιδανικά και εκ φύσεως οτιδήποτε μπορεί να μεταφραστεί σε μαθηματικά. Δηλαδή τα πάντα αν ρωτήσεις έναν μαθηματικό. Αλλά στην προκειμένη περίπτωση ειδικά εκεί που τα μαθηματικά προβλήματα μοιάζουν άλυτα με τις συμβατικές μεθόδους. Έτσι οι πρώτες πρακτικές εφαρμογές εμπίπτουν ήδη σε τρεις βασικές κατηγορίες: τις προσομοιώσεις, τη βελτιστοποίηση και τη μηχανική μάθηση.

Προσομοίωση του μικρόκοσμου: ειδικά υλικών της δομής τους και σε μοριακό επίπεδο είναι ίσως το πιο πολλά υποσχόμενο πεδίο μετά την κυβερνοασφάλεια την

ΚΒΑΝΤΙΚΗ ΑΝΑΣΦΑΛΕΙΑ;

Τι θα γίνει σε έναν κόσμο όπου κβαντικοί υπερυπολογιστές σε χέρια λίγων θα μπορούν θεωρητικά να «σπάνε»... τα πάντα; Απευθυνθήκαμε στη Ντίνα Συντίλα, Πρόεδρο ΔΣ του ISC2 Hellenic Chapter και τον Γιάννη Ηλιάδη, Πρόεδρο της Επιτροπής Ελέγχου του για να μας εξηγήσουν την πραγματική φύση της κβαντικής υπολογιστικής σε ό,τι αφορά την κυβερνοασφάλεια.

Και αυτοί κατέφυγαν στον Robert Louis Stevenson: «Dr. Jekyll και Mr. Hyde! Ο κβαντικός Mr. Hyde κυκλοφορεί στις σκιές με μια κρυπταναλυτική βαριοπούλα στο χέρι, ενώ ο κβαντικός Dr. Jekyll μας προσφέρει ένα προηγμένο οπλοστάσιο αλγοριθμικής άμυνας. Πώς ισορροπούμε τη διπλή προσωπικότητα; Αλλά πριν ας αναρωτηθούμε: Τα μαθηματικά τρέχουν ταχύτερα από το hardware; Η κατασκευή ενός κβαντικού υπολογιστή εκατομμυρίων φυσικών qubits είναι ένας μηχανικός άθλος και αποτελεί μεγάλο εμπόδιο στην ευρεία υλοποίηση κβαντικών εφαρμογών.
Τα τελευταία χρόνια, η αλγοριθμική έρευνα συμπίεσε τις απαιτήσεις hardware πολύ ταχύτερα από όσο αναμενόταν, μειώνοντας τις απαιτήσεις σε φυσικά qubits και φέρνοντας χρονικά πιο κοντά την πρακτική εφαρμογή. Ας σταχυολογήσουμε τις πρόσφατες εξελίξεις:

- **Αύγουστος 2023:** Ο Oded Regev παρουσιάζει πολυδιάστατη παραλλαγή του αλγορίθμου Shor, μειώνοντας τον αριθμό των απαιτούμενων κβαντικών πυλών για την παραγοντοποίηση.
- **Οκτώβριος 2023:** Οι Ragavan και Vaikuntanathan μειώνουν περαιτέρω τις απαιτήσεις της μεθόδου Regev και οι Ekera και Gartner επεκτείνουν τη μέθοδο Regev για τον υπολογισμό διακριτών λογαρίθμων.
- **Μάρτιος 2026:** Οι Chevignard, Fouque και Schrottenloher εκτίμησαν (υπό παραδοχές) ότι το Elliptic Curve Discrete Logarithm Problem για μια καμπύλη 256-bit λύνεται με μόλις 1.193 λογικά qubits.

Δύο κύριες απειλές δεν αποτελούν -πλέον- υποθετικά σενάρια επόμενης δεκαετίας. Αφενός το Harvest Now, Decrypt Later (HNDL): κρυπτογραφημένη πληροφορία που υποκλέπτεται σήμερα (π.χ. TLS, VPN) μπορεί να αποκρυπτογραφηθεί στα επόμενα λίγα χρόνια. Αφετέρου το Trust Now, Forge Later (TNFL): ψηφιακές υπογραφές επί firmware, bootloaders θα είναι τεχνικά εφικτό να πλαστογραφηθούν, διαρρηγνύοντας το root of trust και επιφέροντας μη ιχνηλάσιμο πλήγμα στην ακεραιότητα συστημάτων».

ΑΝΕΛΠΙΣΤΟ ΚΒΑΝΤΙΚΟ ΑΜΥΝΤΙΚΟ ΟΠΛΟΣΤΑΣΙΟ

«Οι ερευνητικές εξελίξεις δημιουργούν νέα όπλα κυβερνοάμυνας, απολύτως αναγκαία για το εγγύς μέλλον. Εντροπία Τώρα! Οι Κβαντικές Γεννήτριες Τυχαίων Αριθμών (QRNG) προσφέρουν εντυπωσιακή εντροπία. Έχει ήδη επιτευχθεί ενσωμάτωση QRNG στο OpenSSL για το TLS, ενώ PQC αλγόριθμοι τροποποιήθηκαν ώστε να αντλούν εντροπία αποκλειστικά από κβαντικές πηγές.
Στην post-quantum εποχή, το key establishment βασίζεται σε PQC, σύμφωνα με την κοινή θέση των ANSSI, BSI και NLNCSA. Υπάρχουν μηχανισμοί ανθεκτικοί σε κβαντικές επιθέσεις, όπως τα PQC KEMs. Παράλληλα, η Quantum Key Distribution (QKD) μπορεί να λειτουργήσει συμπληρωματικά προς την PQC, υπό προϋποθέσεις ύπαρξης υποδομών που δεν είναι ευρέως διαθέσιμες. Η Ευρώπη επενδύει στην ανάπτυξη αυτής της συμπληρωματικής υποδομής μέσω του EuroQCI, με χαρακτηριστικά παραδείγματα το Rome QMAN και τις ελληνικές δοκιμές επίγειων και δορυφορικών συστημάτων HellasQCI.
Πρόσφατη πρόταση για ένα Quantum Enhanced Adaptive Defense System (QEAD) συνδυάζει κλασικά μοντέλα με παραμετροποιήσιμα κβαντικά κυκλώματα, ώστε να βελτιώνει σε πραγματικό χρόνο την ανίχνευση επιθέσεων με reinforcement learning. Σε συνθετικό dataset, το σύστημα εντόπισε το 42,7% των zero-day attack samples (zero-day recall), έναντι 3,3% που πέτυχε το Isolation Forest».

ΕΜΕΙΣ ΤΙ ΚΑΝΟΥΜΕ;

«Πρώτον: βαθιά ανάσα. Ο εχθρός είναι προ των πυλών, αλλά προλαβαίνουμε — αρκεί να ξεκινήσουμε από τα σωστά βήματα.
Χαρτογραφήστε. Cryptographic Bill of Materials (CBOM): πού υπάρχει RSA, ECC; Συμπληρώστε με dependency maps — εσωτερικές και τρίτων — και διάλογο με την εφοδιαστική αλυσίδα. Είναι το δυσκολότερο βήμα και το ακριβότερο αν καθυστερήσει. Η εμπειρία του Y2K έδειξε ότι το μεγαλύτερο κόστος αφορά τον εντοπισμό, όχι στη διόρθωση.
Προτεραιοποιήστε με βάση τον κίνδυνο. Αν το άθροισμα διάρκειας ζωής δεδομένων και χρόνου μετάπτωσης υπερβαίνει τον χρόνο έως τον κβαντικό υπολογιστή, η μετάβασή σας σε PQC πρέπει να έχει ήδη ξεκινήσει (ανισότητα Mosca).
Αναπτύξτε υβριδικά (X25519 + ML-KEM-768), κατά ANSSI και BSI. Προσοχή: hybrid σημαίνει AND, όχι OR — ώστε να καλύπτεστε ταυτόχρονα από την κβαντική απειλή και από αστοχίες των πρώιμων PQC αλγορίθμων.
Διαχειριστείτε την αλλαγή. Είναι θέμα αρχιτεκτονικής και κύκλου ζωής, το οποίο απαιτεί προϋπολογισμό και υψηλή τεχνογνωσία. Δεν αλλάζει μόνο ο αλγόριθμος, αλλά τα μεγέθη: μια υπογραφή ML-DSA-87 καταλαμβάνει 4.627 bytes, έναντι 64 της ECDSA. Τα μεγέθη επηρεάζουν δίκτυο, πιστοποιητικά, μνήμη συσκευών, trust anchors στο hardware και, τέλος, τη διαθεσιμότητα της υπηρεσίας.
Μην επαναπαύεστε. Η ανακοίνωση της Anthropic (Ιούλιος 2026) ότι το Claude Mythos Preview εντόπισε ευπάθεια στο υπό τυποποίηση HAWK — lattice-based υπογραφή, υποψήφια του NIST μέχρι τον Ιούλιο 2026 — αποδεικνύει πόσο εύκολα ανατρέπονται οι μαθηματικές παραδοχές μας στη νέα εποχή.
Η συνταγή: ξεκινήστε τις προληπτικές ενέργειες τώρα, προτού ο Mr. Hyde αρχίσει να ισιώνει τις ελλειπτικές καμπύλες μας με την κβαντική βαριοπούλα του».

οποία όμως θα αφήσουμε για το τέλος. Τα κλασικά υπολογιστικά συστήματα δεν μπορούν να μοντελοποιήσουν τη συμπεριφορά περίπλοκων μοριακών δομών λόγω των άπειρων πρακτικά μεταβλητών που αυξάνονται εκθετικά ανάλογα με το μέγεθος των συστημάτων που εξετάζονται. Οι κβαντικοί υπολογιστές λειτουργούν με τις ίδιες «χαοτικές» αρχές. Και αυτό τους κάνει εξαιρετικά πολλά υποσχόμενους για ιατρική έρευνα, ανάπτυξη φαρμάκων από φαρμακευτικές εταιρείες, τη χημική μηχανική και τις προκλήσεις της όπως την ανάπτυξη νέων μπαταριών που θα σπάσουν τα όρια της ηλεκτροκίνησης, αλλά και τη δημιουργία νέων σύνθετων υλικών.

Ο οικονομικός κλάδος: Η έρευνα της IBM «Exploring Quantum Computing Use Cases for Financial Services» έχει ήδη αναδείξει τους στόχους για το κβαντικό οπλοστάσιο στο fintech. Οι δύο βασικότεροι -και όχι τυχαία εξαιρετικά προσοδοφόροι- είναι η πρόβλεψη με προηγμένα μαθηματικά μοντέλα του επενδυτικού και ασφαλιστικού κινδύνου και η βελτιστοποίηση του trading. Η αναβάθμιση της προσομοίωσης κινδύνων σημαίνει βελτιστοποίηση των επενδυτικών στρατηγικών και η δυνατότητα να γίνει αυτό σε πρωτοφανή κλίμακα και ταχύτητα αναμένεται να αλλάξει ολόκληρο το οικονομικό και ασφαλιστικό οικοσύστημα. Σε βαθμό που η IBM έχει ήδη επενδύσει σε ανάλογες εφαρμογές κβαντικής τεχνολογίας, σε συνεργασία με την Vanguard, ξεκινώντας μάλιστα δοκιμές με portfolio optimization σε συνθήκες της πραγματικής αγοράς.

Βιομηχανία: Το τρίτο πεδίο εφαρμογής είναι η βελτιστοποίηση της βιομηχανίας. Κατασκευαστές, εταιρείες logistics και ενεργειακοί πάροχοι ήδη ποντάρουν και δοκιμάζουν εκεί που ελπίζουν να προκύψει το κέρδος: σε προβλήματα που εμπλέκουν υπερπολλαπλές μεταβλητές αλλά η λύση τους θα έχει σοβαρή επίπτωση στη μείωση του λειτουργικού κόστους. Δρομολόγηση οχημάτων και παραγγελιών, επανασχεδίαση της αλυσίδας παραγωγής, προμήθειας και μεταφοράς, προγραμματισμός smart factories και έξυπνη διαχείριση των μονάδων παραγωγής ηλεκτρικής ενέργειας και των δικτύων διανομής της. Και σε επόμενο επίπεδο η "αλγοριθμική" διαχείριση όλων αυτών σε συνδυασμό και σε πραγματικό χρόνο.

Ασφάλεια: Όπως είναι αναμενόμενο το πιο καυτό ζήτημα της κβαντικής κρυπτογράφησης και αποκρυπτογράφησης συμπίπτει με την «αγορά» στην οποία το κόστος δεν είναι ζήτημα, δηλαδή αυτή της άμυνας και της ασφάλειας. Η αγία τριάδα των early adopters με «θαυματουργό» budget είναι και στην κβαντική υπολογιστική «τηλεπικοινωνίες, στρατός, κυβέρνηση» και η συγκεκριμένη δυναμική αξίζει τη δική της ενότητα, (η οποία θα ανοίξει στη συνέχεια).

Παρόλα αυτά και όπως επισημαίνει και η φετινή μελέτη της Deloitte, «Quantum Computing Readiness: Quantum Computing Is Coming. Here's How to Reduce Expensive Guesswork to Build Business Value Now», το όνομα του παιχνιδιού προς το παρόν είναι ο πειραματισμός και θα χρειαστούν μερικά ακόμα χρόνια του quantum computing στο δοκιμαστικό σωλήνα πριν περάσουμε σε ευρεία εμπορική χρήση.

QUANTUM ΧΩΡΙΣ QUANTUM COMPUTER

Ηλίας Κ. Σάββας, Καθηγητής του Τμήματος Ψηφιακών Συστημάτων στο Πανεπιστήμιο Θεσσαλίας

«Θα γίνει, λοιπόν, η κβαντική υπολογιστική μαζικά προσβάσιμη; Πιθανότατα όχι με τον ίδιο τρόπο που έγινε το smartphone ή ο προσωπικός υπολογιστής. Το ίδιο το κβαντικό υλικό θα παραμείνει για αρκετό καιρό εξαιρετικά σύνθετο και ακριβό. Αυτό όμως δεν σημαίνει ότι η τεχνολογία θα είναι απρόσιτη. Η πρόσβαση μέσω Quantum Computing as a Service (QCaaS) επιτρέπει ήδη σε ερευνητές, φοιτητές και επιχειρήσεις να πειραματίζονται με πραγματικούς κβαντικούς υπολογιστές μέσω του υπολογιστικού νέφους. Ίσως, επομένως, το σημαντικότερο ερώτημα δεν είναι αν όλοι θα αποκτήσουμε έναν κβαντικό υπολογιστή στο σπίτι. Είναι αν θα είμαστε έτοιμοι να κατανοήσουμε, να προγραμματίσουμε και να αξιοποιήσουμε αυτή τη νέα τεχνολογία όταν ωριμάσει. Και σε αυτό το σημείο η εκπαίδευση και η επένδυση στους νέους ερευνητές είναι ίσως η σημαντικότερη κβαντική επένδυση που μπορούμε να κάνουμε σήμερα».

Στα επόμενα κβαντικά επεισόδια...

Τι πρέπει να περιμένουμε στο άμεσο μέλλον; «Το επόμενο μεγάλο βήμα είναι η μετάβαση από τους σημερινούς θορυβώδεις κβαντικούς υπολογιστές της εποχής NISQ σε fault-tolerant κβαντικούς υπολογιστές, ικανούς να εκτελούν πολύ μεγαλύτερους και αξιόπιστους υπολογισμούς» μας λέει ο Ηλίας Σάββας. «Η αύξηση του αριθμού και της ποιότητας των φυσικών και λογικών qubits, η αποτελεσματική διόρθωση κβαντικών σφαλμάτων και η βελτίωση των κβαντικών πυλών αποτελούν κρίσιμες προϋποθέσεις. Εξίσου σημαντική θα είναι η ανάπτυξη υβριδικών αρχιτεκτονικών, στις οποίες κλασικοί και κβαντικοί υπολογιστές θα συνεργάζονται».

Τα qubits είναι εξαιρετικά ευαίσθητα στις περιβαλλοντικές παρεμβολές και για να έχουν αξιόπιστα αποτελέσματα πρέπει ένα σύστημα να τσεκάρει όλα τα αποτελέσματα ενός κβαντικού υπολογιστικού συστήματος για τέτοια λάθη και μάλιστα με ρυθμό μεγαλύτερο από όσο ένα τόσο γρήγορο σύστημα μπορεί να τα δημιουργεί. Γι' αυτό και το οικοσύστημα δημιουργών κβαντικών συστημάτων μετατοπίζει την προσοχή του από την απλή αύξηση του αριθμού των φυσικών qubits στην παραγωγή πιο αξιόπιστων συστημάτων και τελικά «λογικών qubits», δηλαδή ομάδων φυσικών qubits που συνεργάζονται για να δημιουργήσουν μια πιο σταθερή υπολογιστική μονάδα. Το Quantum Technology Monitor 2025 της McKinsey αναγνωρίζει αυτή τη μετατόπιση προς τη σταθεροποίηση των qubits ως ένα σημαντικό σημείο καμπής για τη βιομηχανία και αρκετές από τις πρόσφατες ▶

Η μακροχρόνια ισχύς των ψηφιακών υπογραφών και σφραγίδων

Η κβαντική απειλή αφορά ολόκληρη την αλυσίδα εμπιστοσύνης. Ηλεκτρονικές υπογραφές, σφραγίδες και χρονοσφραγίδες βασίζονται σε κλειδιά και αλγορίθμους που σύντομα θα θεωρούνται ευάλωτοι. Η προστασία των σημερινών εγγράφων πρέπει επομένως να αρχίσει πριν αυτοί πάψουν να θεωρούνται ασφαλείς.

Η απειλή για τα υφιστάμενα έγγραφα

Δανειακές συμβάσεις, τίτλοι ιδιοκτησίας, εταιρικά πρακτικά και δημόσιες συμβάσεις υπογράφονται σήμερα με αλγορίθμους όπως RSA και ECC. Ένας επαρκώς ισχυρός κβαντικός υπολογιστής θα μπορούσε μελλοντικά να καταστήσει εφικτή την πλαστογράφηση υπογραφών που βασίζονται σε αυτούς.

Αυτό δεν ακυρώνει αυτομάτως τη νομική ισχύ μιας εγκεκριμένης ηλεκτρονικής υπογραφής. Μπορεί όμως να υπονομεύσει τη δυνατότητα απόδειξης ότι η υπογραφή ήταν έγκυρη και το έγγραφο ακέραιο όταν δημιουργήθηκε. Η μετάβαση σε μετακβαντικούς αλγορίθμους για τις νέες υπογραφές δεν προστατεύει από μόνη της το ήδη υπογεγραμμένο αρχείο.

Η διαφύλαξη αρχίζει σήμερα

Ο eIDAS προβλέπει εγκεκριμένη υπηρεσία διαφύλαξης για εγκεκριμένες ηλεκτρονικές υπογραφές και σφραγίδες, ώστε να επεκτείνεται η αξιοπιστία τους πέραν της περιόδου τεχνολογικής ισχύος. Η διαδικασία πρέπει να ξεκινήσει όσο οι αρχικοί αλγόριθμοι, τα πιστοποιητικά και οι πληροφορίες ανάκλησης παραμένουν αξιόπιστα. Κατά την ένταξη ενός εγγράφου, η υπηρεσία καταγράφει το αποτέλεσμα επικύρωσης της υπογραφής ή της σφραγίδας, συλλέγει τα πιστοποιητικά, τις πληροφορίες ανάκλησης και τα λοιπά δεδομένα επικύρωσης και δημιουργεί αποδεικτικό διαφύλαξης. Το αποδεικτικό προστατεύει το έγγραφο και τεκμηριώνει την κατάσταση της υπογραφής τη συγκεκριμένη χρονική στιγμή.

Η αλυσίδα διαδοχικής προστασίας

Πριν λήξει ένα πιστοποιητικό ή πάψουν να θεωρούνται επαρκή το μήκος του κλειδιού, ο αλγόριθμος υπογραφής ή η συνάρτηση κατακερματισμού που προστατεύουν το αποδεικτικό, η υπηρεσία προσθέτει ένα νέο επίπεδο προστασίας. Το νέο αποδεικτικό καλύπτει το αρχικό έγγραφο και ολόκληρη την προηγούμενη αλυσίδα, χρησιμοποιώντας νέο κλειδί, νέο πιστοποιητικό και ισχυρότερους αλγορίθμους.

Δεν αντικαθίσταται η αρχική υπογραφή του χρήστη. Διατηρείται και περιβάλλεται από διαδοχικά επαληθεύσιμα αποδεικτικά. Επειδή κάθε νέο επίπεδο δημιουργείται όσο το προηγούμενο παραμένει αξιόπιστο, μπορεί αργότερα να αποδειχθεί ότι η αρχική υπογραφή ήταν έγκυρη πριν ο αλγόριθμός της καταστεί ευάλωτος.

Κώστας Νούσιας, ***Trust Services Director, ADACOM***

Η ΚΒΑΝΤΙΚΗ ΑΠΕΙΛΗ ΔΕΝ ΑΦΟΡΑ ΜΟΝΟ ΤΟ ΑΥΡΙΟ: Η ΑΞΙΟΠΙΣΤΙΑ ΤΩΝ ΣΗΜΕΡΙΝΩΝ ΨΗΦΙΑΚΩΝ ΥΠΟΓΡΑΦΩΝ ΠΡΕΠΕΙ ΝΑ ΠΡΟΣΤΑΤΕΥΤΕΙ ΑΠΟ ΣΗΜΕΡΑ

Η χρονοσφραγίδα χρειάζεται επίσης διαφύλαξη

Η χρονοσφραγίδα αποδεικνύει ότι τα προστατευόμενα δεδομένα υπήρχαν σε συγκεκριμένο χρόνο, αλλά δεν είναι διαχρονικά άτρωτη. Βασίζεται και αυτή σε κρυπτογραφικό κλειδί, πιστοποιητικό, αλγόριθμο υπογραφής και συνάρτηση κατακερματισμού. Γι' αυτό ανανεώνεται πριν αποδυναμωθούν οι μηχανισμοί της, ώστε η νέα χρονοσφραγίδα να προστατεύει και την προηγούμενη.

Ο ρόλος του Εγκεκριμένου Παρόχου Υπηρεσιών Εμπιστοσύνης (QTSP)

Η εγκεκριμένη διαφύλαξη παρέχεται μόνο από QTSP που διαθέτει το αντίστοιχο εγκεκριμένο καθεστώς για τη συγκεκριμένη υπηρεσία. Η συμμόρφωση με πρότυπα όπως ETSI TS 119 511 και ETSI TS 119 512, η συνεχής κρυπτογραφική παρακολούθηση και η έγκαιρη ανανέωση των αποδεικτικών είναι αυτά που διατηρούν την αξιοπιστία των υπογραφών και σφραγίδων για 10, 20 ή 30 χρόνια.

Για τους οργανισμούς, η απόφαση δεν είναι απλώς πού θα αποθηκεύσουν τα έγγραφά τους, αλλά πώς θα μπορούν να αποδεικνύουν την προέλευση, την ακεραιότητα και την εγκυρότητά τους όταν η σημερινή τεχνολογία δεν θα θεωρείται πλέον ασφαλής.

INFO

Κρέοντος 25, Αθήνα 104 42
T: +30 2105193700
E: info@adacom.com
W: www.adacom.com

ADACOM
SECURITY BUILT ON TRUST

Σε βιομηχανία, finance και κυβερνοασφάλεια, η κβαντική υπολογιστική κάνει ήδη τα πρώτα βήματα από τη θεωρία στην πρακτική εφαρμογή

εξελίξεις επιβεβαιώνουν αυτή την κβαντική «κόντρα». Το τσιπ Willow της Google Quantum AI, που παρουσιάστηκε το 2024, ανέφερε προόδους στη διόρθωση κβαντικών σφαλμάτων χρησιμοποιώντας έναν επεξεργαστή 105 qubit. Ενώ η Microsoft παρουσίασε τον επεξεργαστή Majorana 1 το 2025, βασισμένο σε μια τοπολογική προσέγγιση qubit που έχει σχεδιαστεί για να δημιουργήσει μια πιο κλιμακωτή πορεία προς την ανεκτικότητα σε σφάλματα υπολογισμού. Και παράλληλα η IBM ακολουθεί μια διαφορετική στρατηγική που επικεντρώνεται στην κλιμάκωση υπεραγώγιμων κβαντικών συστημάτων και στην ενσωμάτωση κβαντικών επεξεργαστών με κλασική υπολογιστική υποδομή, ενώ τα δημοσιευμένα σχέδια της εταιρείας περιλαμβάνουν το Blue Jay, ένα σύστημα σχεδιασμένο για να υποστηρίζει κβαντικές λειτουργίες μεγάλης κλίμακας.

Το επόμενο στάδιο είναι επομένως πιθανό να περιλαμβάνει τρεις ταυτόχρονες εξελίξεις: βελτιωμένη διόρθωση σφαλμάτων, πιο εξελιγμένους υβριδικούς κβαντο-κλασικούς αλγόριθμους και ολοένα και πιο αυστηρή συγκριτική αξιολόγηση. Ένα καλό παράδειγμα είναι η πρόσφατη εργασία της IBM στο QOBLIB, ένα πλαίσιο συγκριτικής αξιολόγησης που αποσκοπεί στον εντοπισμό των σημείων όπου η κβαντική βελτιστοποίηση μπορεί να επιδείξει πρακτική αξία πέρα από τις εργαστηριακές επιδείξεις.

Και με το AI; Τι γίνεται στο κομμάτι της αλληλεπίδρασης των κβαντικών υπολογιστών με την τεχνολογία που κυριαρχεί στο προσκήνιο, την ειδησεογραφία και τις χρηματοδοτήσεις τα τελευταία χρόνια; «Ίσως η πιο συναρπαστική εξέλιξη να βρίσκεται στη συνάντηση της κβαντικής υπολογιστικής με την τεχνητή νοημοσύνη. Δεν θεωρώ όμως ότι πρέπει να περιμένουμε απλώς "ταχύτερη AI"» προειδοποιεί ο Ηλίας Σάββας. «Η πραγματική πρόκληση είναι να ανακαλύψουμε εάν οι κβαντικές αρχές μπορούν να οδηγήσουν σε νέους τρόπους αναπαράστασης δεδομένων, βελτιστοποίησης και μηχανικής μάθησης. Εάν αυτό επιτευχθεί σε κλίμακα, θα μπορούσε να επηρεάσει πεδία από την ανακάλυψη φαρμάκων, την ιατρική ακριβείας και την επιστήμη των υλικών μέχρι την αντιμετώπιση σύνθετων προβλημάτων βελτιστοποίησης». **NW**