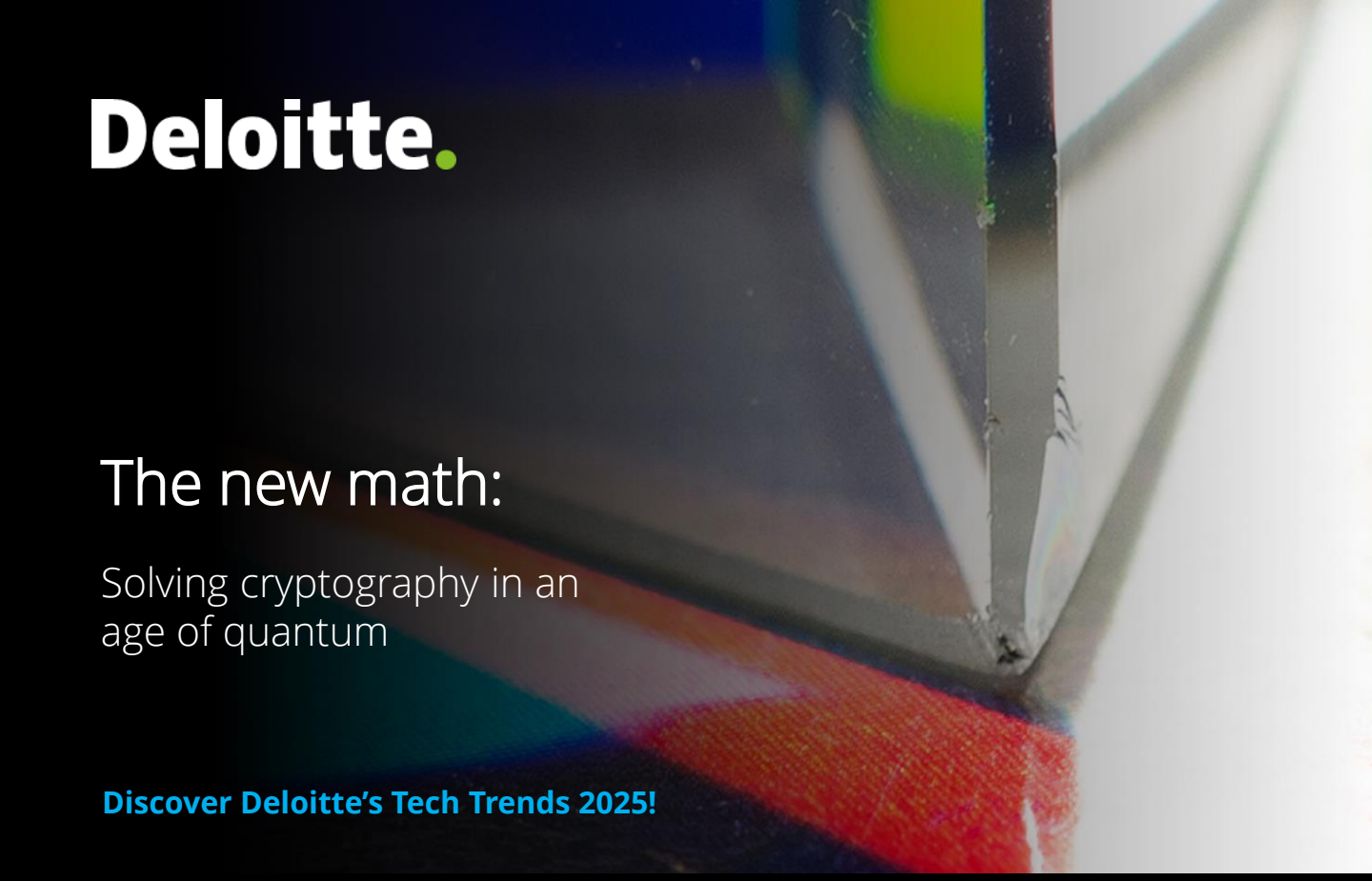

Deloitte.

The new math:

Solving cryptography in an age of quantum

Discover Deloitte's Tech Trends 2025!

As core technology is growing and evolving, due to more powerful hardware and innovation allowing for more computation and AI boosting the productivity of technology workers, IT organizations should investigate another factor hiding just beneath the horizon of their growth path. Deloitte's Tech Trends reports have highlighted in the past the role and importance of security, as the one providing stability.

Safeguarding the Future in the Quantum Era

Today's reliance on data requires not only computational availability but also safeguarding. Data integrity is vital for effective governance, ensuring AI models are trained on accurate information. Likewise, the data confidentiality – whether in transit (such as high-speed trading, diagnostic equipment, or IoT field data) or at rest (like backups, financial models, or transaction records) – is crucial to the stability of our digital economy.

Cryptography, the force behind integrity and confidentiality, is used everywhere. At their core, today's widely trusted encryption schemes rely on mathematical problems (factoring large numbers or solving discrete logarithms) that classical computers cannot solve efficiently. Those traditional methods of safeguarding information are challenged by emerging technologies like quantum computing. While offering unprecedented computational power, it also poses significant risks to current encryption standards. Even our browsers use certain standards to communicate, that are challenged.

The Quantum Challenge

Quantum computers exploit entirely different physics – they operate on the principles of quantum mechanics, enabling them to process complex calculations at speeds, unattainable by classical computers. This capability threatens to undermine the existing encryption methods, potentially exposing sensitive data. For executives, understanding the implications of quantum computing becomes essential to ensure continued protection of organizational assets and maintain stakeholder trust.

The Urgency of Quantum-Resilient Cryptography

Quantum computing is growing at unprecedented speeds. Companies like IBM, Fujitsu, Microsoft but also less well-known companies like Atom are building quantum processors which compute power will overshadow today's best GPU-driven computers with over 1000 qubits per processor already in operation. Moreover, Massachusetts Institute of Technology (MIT) recently revealed new ways of coupling photons and atoms which would shorten the time between computation and readout by a level of magnitude, eliminating one of the bottlenecks of quantum technology growth.

Why does this matter?

The worry is that today's standards, being widely implemented, are not easy to change. Some organizations, due to their technology stack being built over the years, are still suggesting using lower standards, that either do not require much computing power on the end devices or are incompatible with their aging technology stack.

At the same time, cryptographically relevant quantum computers (CRQCs) are expected to break current encryption methods as soon as the 2030s. Reports even suggest that Chinese quantum machines may have already compromised basic algorithms, potentially undermining even the strongest encryption standards like AES.

Path to solution

Fortunately, solutions are emerging. Post-quantum cryptography (PQC) algorithms, recommended by NIST, are being developed to secure key encapsulation and digital signatures, with more innovations underway. As outlined in Deloitte's Tech Trend for 2025 The new math: "The updated NIST standards move away from today's large-number-factoring math problems and leverage lattice and hash problems, which are sufficiently complex to bog down even quantum computers".

However, while quantum computers capable of breaking today's encryption may arrive within 5–10 years, transitioning to quantum-resistant systems could take just as long. This creates a risky window, especially as attackers may already be harvesting encrypted data to decrypt later ("harvest now, decrypt later" attacks). Unlike the Y2K crisis, where the risk was time-bound and predictable, the timeline for CRQCs remains uncertain, causing many organizations to deprioritize preparations despite the potentially massive impact.

Business Implications and Action Plan

To address this threat, organizations should proactively begin transitioning to quantum-resilient cryptographic algorithms that can withstand the capabilities of quantum machines. This involves:

- **Inventory all cryptographic algorithms** in use.
- **Assess the challenges** of implementing new quantum-safe algorithms.
- **Plan necessary hardware and software upgrades** to ensure timely mitigation
- **Invest in quantum-resilient algorithms** to protect against future attacks.
- **Collaborate with cybersecurity experts** for robust security strategies.

Deloitte's commitment to Quantum Security

Deloitte provides strategic guidance, implementation support, and ongoing monitoring to help organizations adapt to the quantum challenges. By partnering with experts, businesses can ensure a secure digital environment moving forward.

Conclusion

While quantum computers promise immense benefits – such as accelerating drug discovery by simulating complex molecules – they also introduce unprecedented security challenges. By embracing quantum-resilient cryptography businesses can protect their data and maintain trust in the digital era.

Embrace this strategic approach not just as a technical necessity, but as an investment in future organizational integrity.

Explore Deloitte's 16th annual Tech Trends report and discover the latest trends: Tech Trends 2025 | Deloitte Insights.

.