

PRESS NOTE

Amaravati, October 15, 2026

SRM AP Hosts National Post-Quantum Cryptography Framework Summit

Every secure transaction in the global digital economy rests on the assumption that the mathematics guarding it will outlast the machines built to break it. Functional quantum systems threaten that assumption, and today's public-key encryption standards would be left exposed. It was against this backdrop that SRM AP hosted a national Stakeholder Consultation Workshop on Post-Quantum Cryptography and Cybersecurity, convened by Amaravati Quantum Valley. The workshop gathered policy-makers, academics and regulators to chart a roadmap for quantum-resistant digital infrastructure, and it served as a platform to align regional deep-tech research with wider global security mandates.

Opening the proceedings, Prof. Ch Satish Kumar, Vice-Chancellor of SRM AP, set out the university's ambition to become a premier global research hub. He noted that the campus was among the earliest academic centres to establish a dedicated base for quantum technological infrastructure, and that its modern facilities and open collaboration models are designed to nurture international industry-academia partnerships. In doing so, the university seeks to help India emerge as a global leader in cryptographic resilience, contributing the foundational research needed to safeguard data networks the world over.

The wider vision behind the gathering was outlined by Shri CV Sridhar, Managing Director of AP SQM, who traced the origins of the Amaravati Quantum Valley initiative. Launched last year to cultivate a robust quantum hardware ecosystem, the project recruits startups and connects directly with advanced computing infrastructure, including the IIT Madras quantum network and IBM quantum platforms. Anchored by the Amaravati Quantum Valley Declaration, its roadmap spans photonic Ising machines, an expanded Quantum and AI Innovation Centre hub, advances in precision oncology and indigenous hardware manufacturing capable of competing on the global stage.

Regulatory clarity was given by Dr Sudeep Oberai, Chairman of the MeitY Expert Committee on Post-Quantum Cryptography, who addressed the policy challenges confronting the nation. The committee was constituted in May by the Ministry of Electronics and Information Technology through the Office of the Controller of Certifying Authorities, and is charged with evaluating algorithm readiness and establishing national security baselines, particularly for digital certificates and signatures. Dr Sudeep Oberai observed that Indian education has traditionally prized individual achievement over the collaborative frameworks that global standards demand, and that this orientation will need to shift. Drawing a parallel with the original digital signature mandates under the IT Act, he described how the committee is assessing vulnerabilities across the ecosystem and helping token manufacturers, banks and software vendors adapt before legacy systems are compromised.

The interactive session that followed brought the discussion from principle to practice, with contributions from financial and technology stakeholders already preparing for implementation. Delegates from Punjab National Bank described their progress within the Reserve Bank of India's cybersecurity framework, sharing migration roadmaps, latency considerations and lessons drawn from specialised hackathons.

Leaders from Quantum AI Global presented solutions including Q Forte, Q Sleeve and Quantum Random Number Generators, cautioning that partial upgrades leave backend systems open to global cyber threats. Supported by insights from MeitY scientists Dr KK Soundra Pandian and Shri P Ramachandran, the workshop set out clear requirements for quantum-certifiable hardware and strengthened the standing of SRM University-AP and Amaravati Quantum Valley as key conveners in the pursuit of global quantum security.