

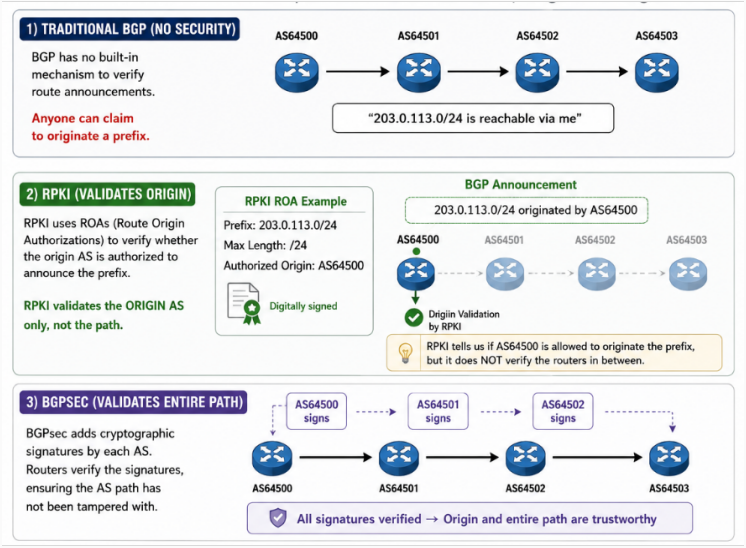
afnic
Internet
made in France

PQC Webinar - 15/06/2026

The Quantum Transition: What It Means for Routing Security

– *Sandoche BALAKRICHENAN*

How RPKI & BGPsec improve routing security



Routing Security Depends on Asymmetric Cryptography

RPKI • ROAs • BGPsec

⇓

Digital Signatures

⇓

RSA ECDSA ECC

⇓

Asymmetric Cryptography

How Quantum Computers break RSA - Simple overview

- RSA's security relies on the difficulty of prime factorization.
  - If n ='21' => Prime factors are 'p'(3) * 'q'(7)
  - Once n = p*q is factored -> attacker reconstructs the private key (d).

- Classical computers cannot factor 2048 bit numbers in reasonable time.
  - n = '32452843... (617 digits long)'
  - $\approx 10^{615}$ possible primes to test n

- Quantum Computers running Shor's algorithm could factor 'n' in hours to days .

Preparing Routing Security for the Quantum Era

1. Identify cryptographic dependencies (RPKI certificates, ROAs, BGPsec signatures).
2. Evaluate post-quantum alternatives.
3. Plan hybrid deployments (Classical + Post-Quantum).
4. Assess operational impact (repository size, bandwidth, validation overhead).
5. Develop a gradual migration strategy.

Thank You

Contact: sandoche.balakrichenan@afnic.fr

Questions?