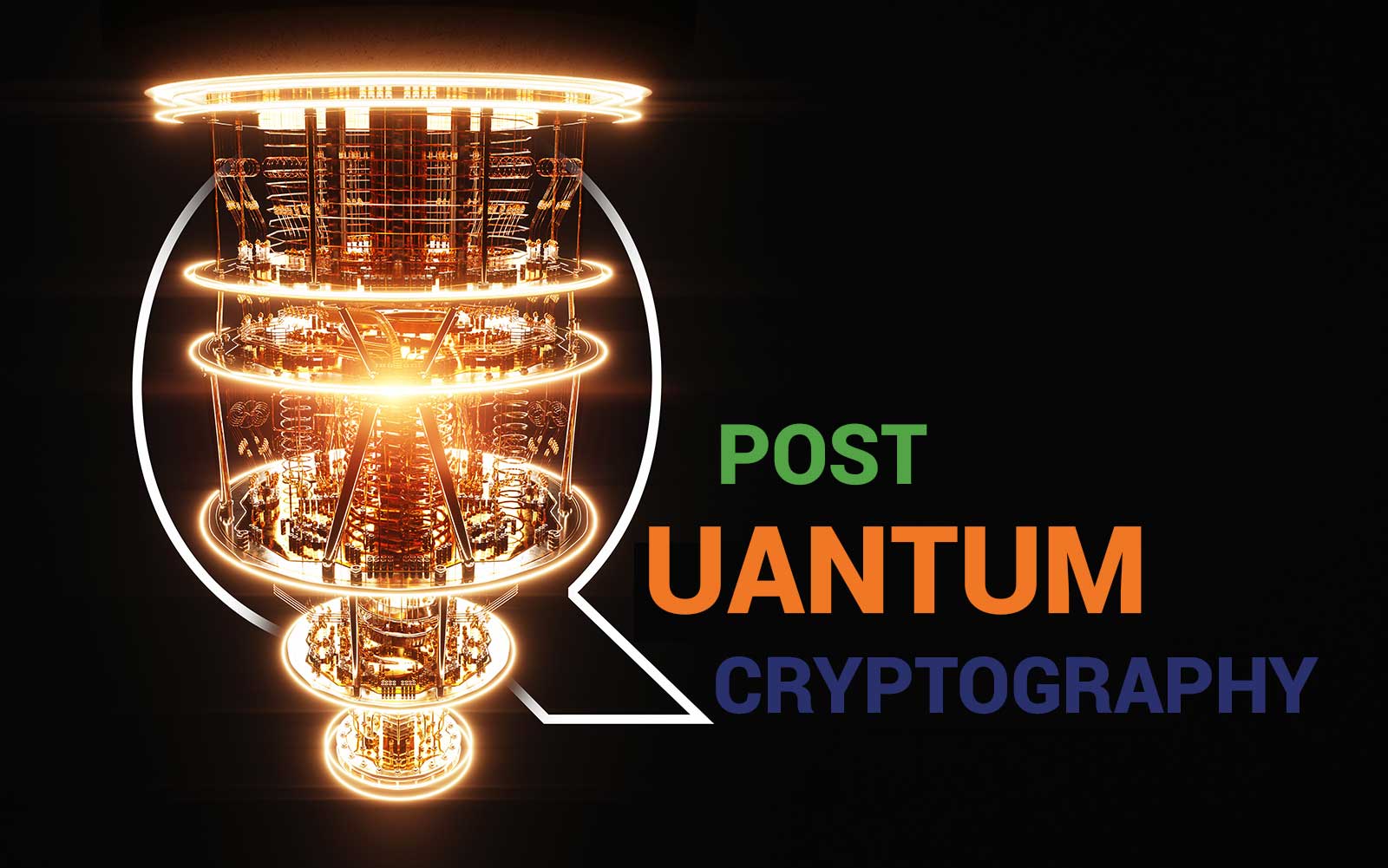
Криптографийн ирээдүй:

Квантын дараах криптографи (PQC)

Квантын компьютерууд хөгжихийн хэрээр криптографийн ландшафт үндсэн өөрчлөлттэй тулгарч байна. RSA болон ECC (Elliptic Curve Cryptography) зэрэг математик хүндрэлүүд боло (том тооны факторизаци хийх, дискрет логарифмууд) суурилсан байдаг ба уламжлалт шифрлэлтийн алгоритмууд нь сонгодог компьютеруудад тооцоолоход хэцүү боловч хангалттай хүчирхэг квант компьютерээр харьцангуй амархан шийдэж болохыг баталсан байдаг.

Пост квант криптографи /квантын дараах криптограф/ (PQC)\*\* нь квант компьютерийн халдлагад тэсвэртэй криптограф алгоритмуудыг боловсруулахад чиглэсэн салбар юм.

NIST нь торонд суурилсан криптограф, хэшт суурилсан гарын үсэг, код дээр суурилсан криптограф\*\* зэрэгт үндэслэн нэр дэвшигчдийг сонгож авсан байдаг.



Энэ онд криптограф судлаачид пост кюант криптографын хөгжүүлэлт, нууцлалын технологи {privacy technologies}, практик хэрэглээний дэвшлээс үүдэлтэй хэд хэдэн гайхалтай зүйлс тохиосон.

* NIST-ийн PQC буюу квант тооцоололд тэсвэртэй алгоритмын сонгон шалгаруулах уралдаан эцсийн шатандаа явагдаж байна..
* Уралдааны сүүлийн шатны алгоритмууд: Kyber болон NTRU алгоритмуудыг нийтийн түлхүүрийн шифрлэлтийн /Publickey encryption/ стандарт алгоритмд, FrodoKEM-ийг түлхүүр солилцох системийн стандартад сонгохоор болоод байна. Эдгээр алгоритмууд нь торны онолд суурилсан /Lattice/ байдаг.
* Квантын аюулгүй түлхүүрийн менежмент: NIST нь мөн түлхүүр солилцооны протоколд зориулсан сонгодог болон квантаас хойшхи криптографийн алгоритмуудыг хослуулсан эрлийз шийдлүүдийг санал болгохоор ажиллаж байна.
* Квант тэсвэртэй тоон гарын үсэг: Хөгжлийн өөр нэг гол талбар бол квантад тэсвэртэй тоон гарын үсэг юм. \*\*SPHINCS+\*\* (хэш-д суурилсан гарын үсэг) болон \*\*Falcon\*\* (торон дээр суурилсан гарын үсгийн схем) зэрэг алгоритмуудыг бодит системд туршиж, хэрэгжүүлж байна.

Нэмж хэлэхэд тус уралдааны PQC стандартчиллын үйл явцыг зургаар харуулав.

