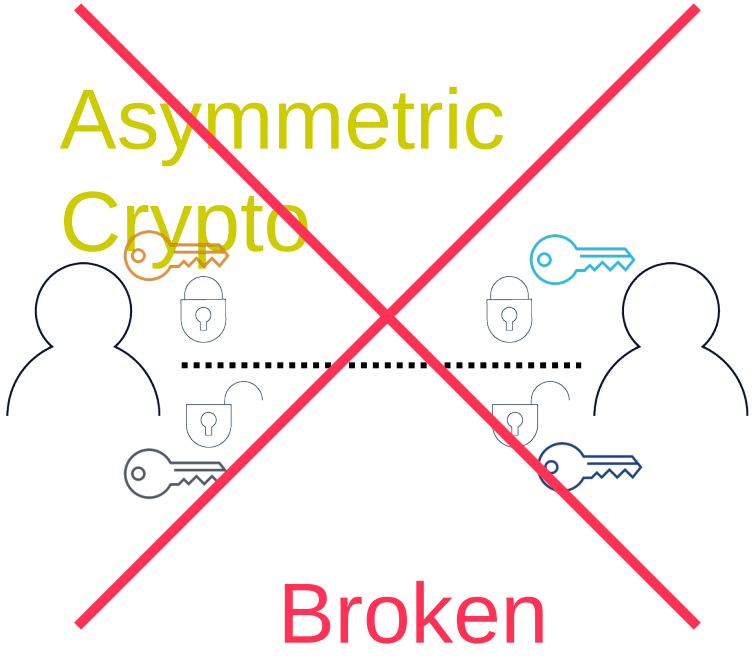
PQ KEMs for COSE AND JOSE

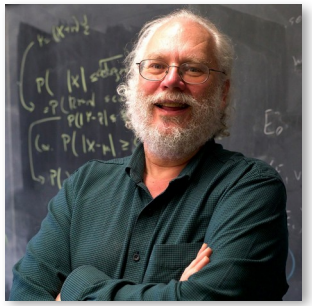
draft-reddy-cose-jose-pqc-kem

Tirumaleswar Reddy, Hannes Tschofenig, Aritra Banerjee

IETF 119, Brisbane

Impact of Quantum Computers in Cryptography

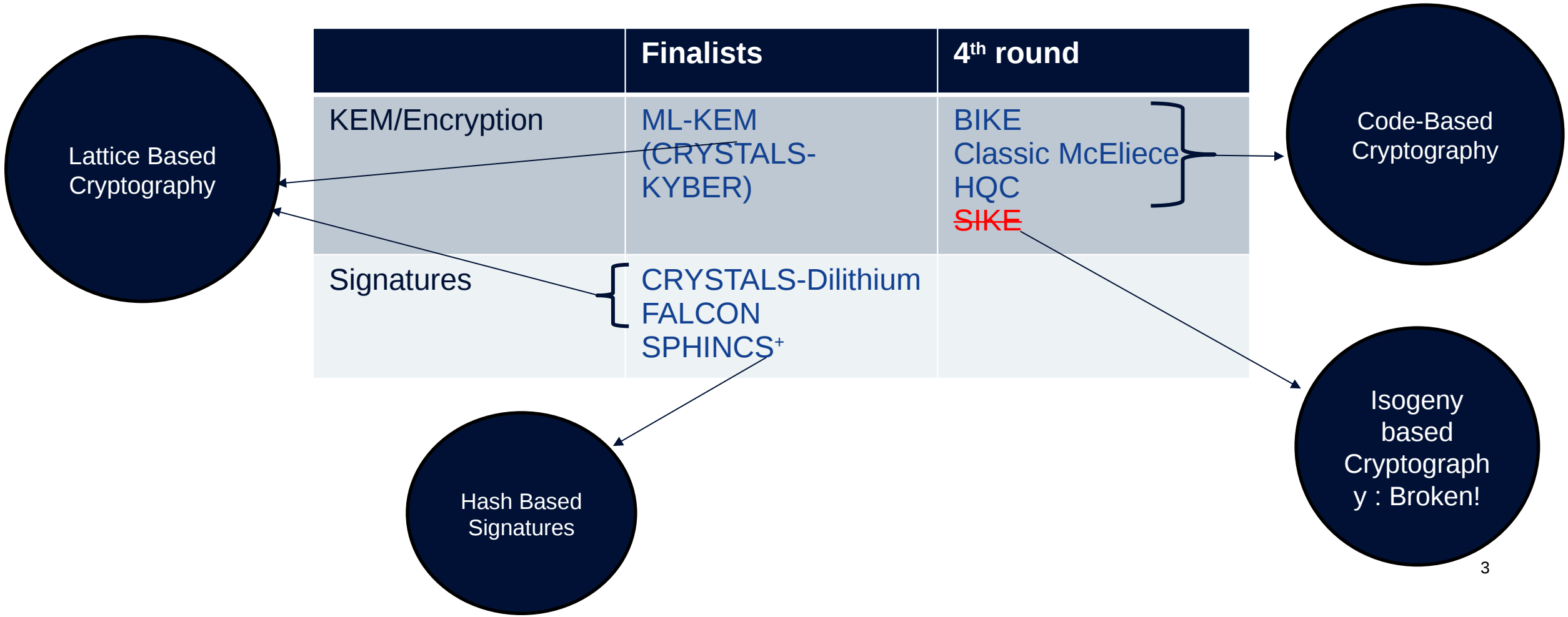




Peter Shor

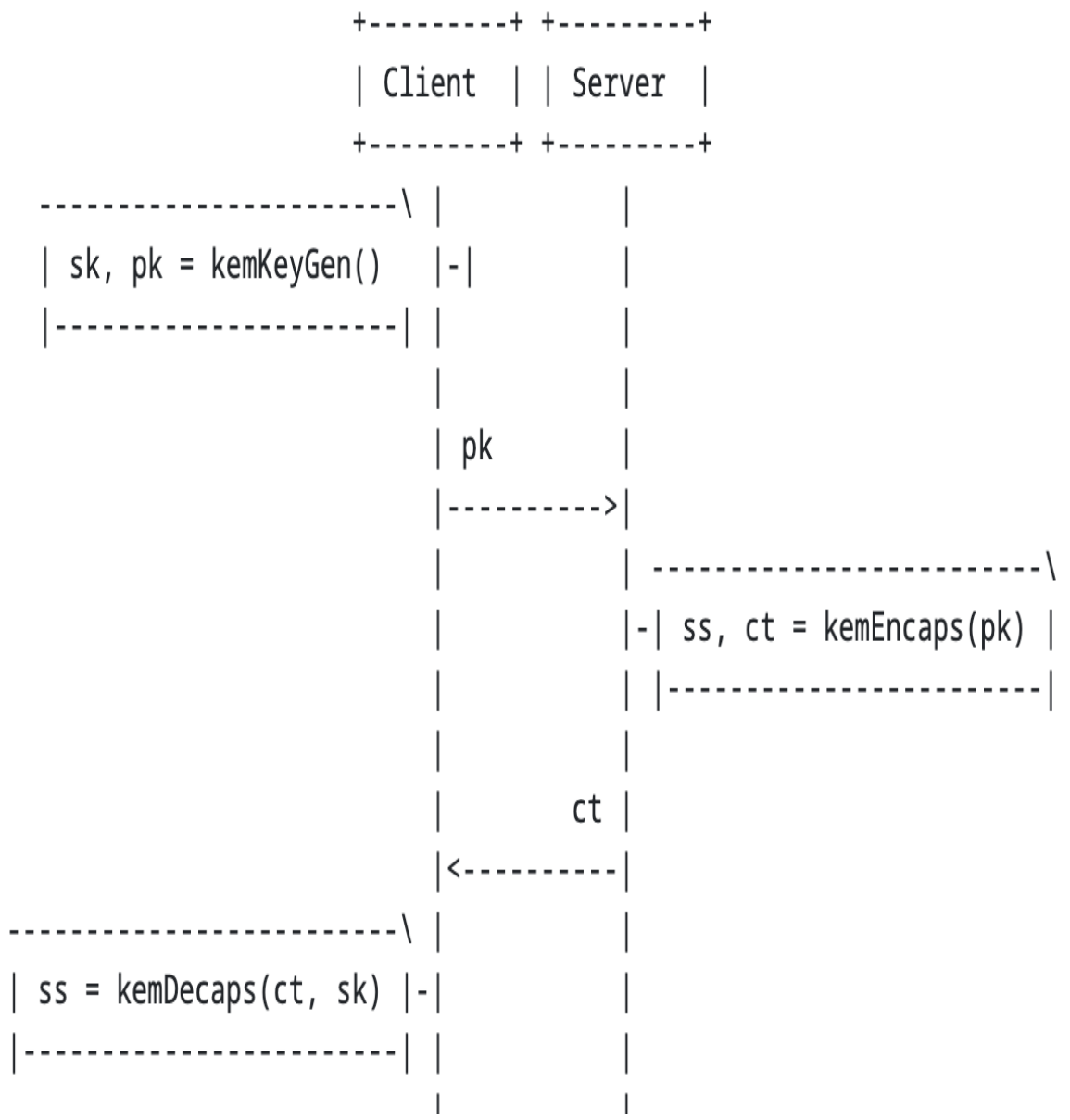
Algorithm for prime factorization of large integers

NIST Candidates Selected for Standardization

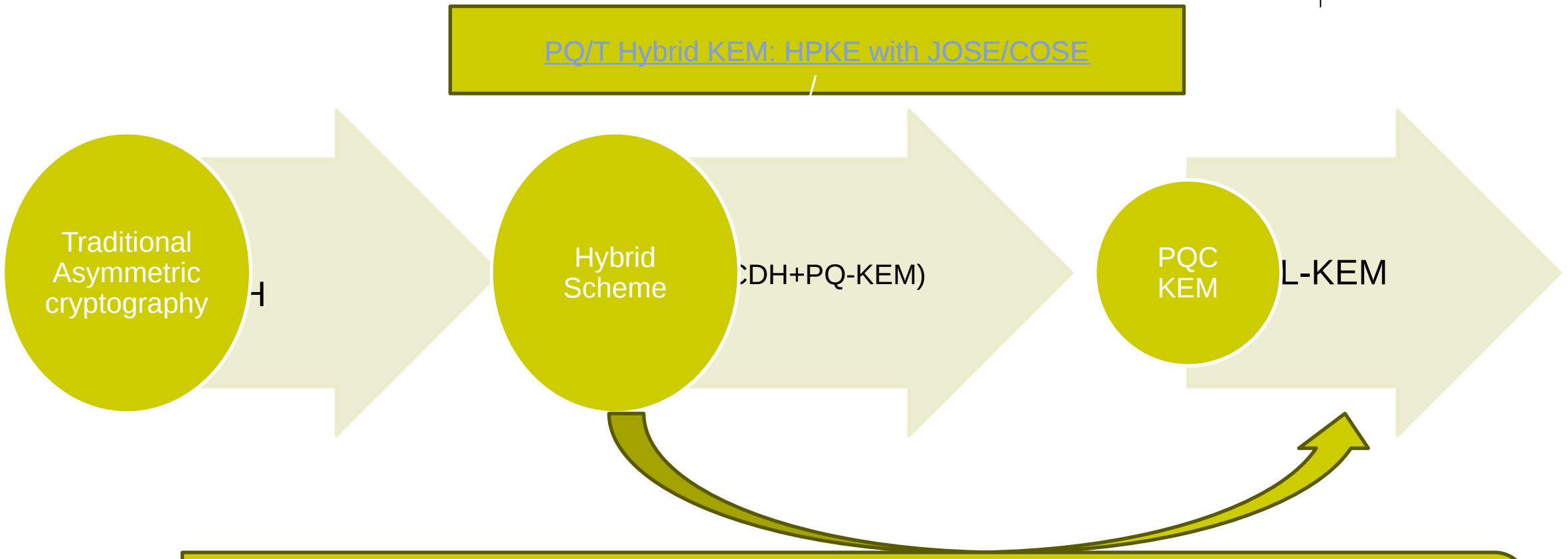


	Finalists	4th round
KEM/Encryption	ML-KEM (~~CRYSTALS-~~KYBER)	BIKE Classic McEliece HQC ~~SIKE~~
Signatures	CRYSTALS-Dilithium FALCON SPHINCS+	

KEM


Client
Server
sk, pk = kemKeyGen()
pk
ss, ct = kemEncaps(pk)
ct
ss = kemDecaps(ct, sk)

Transition path



PQ-KEM Encapsulation

- (SS', CT) = kemEncaps(recipPubKey)
- SS = KDF(SS', SSLen)

PQ-KEM Decapsulation

- SS' = kemDecaps(recipPrivKey, CT)
- SS = KDF(SS', SSLen)

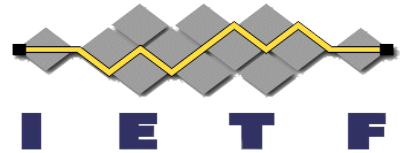
COSE Ciphersuite Registration

JOSE	COSE ID	Description	Recommended
MLKEM512-KMAC128	TBD1	ML-KEM-512 + KMAC128	No
MLKEM768-KMAC256	TBD2	ML-KEM-768 + KMAC256	No
MLKEM1024-KMAC256	TBD3	ML-KEM-1024 + KMAC256	No
MLKEM512-KMAC128+AES128KW	TBD4	ML-KEM-512 + KMAC128 + AES128KW	No
MLKEM768-KMAC256+AES256KW	TBD5	ML-KEM-768 + KMAC256 + AES256KW	No
MLKEM1024-KMAC256+AES256KW	TBD6	ML-KEM-1024 + KMAC256 + AES256KW	No

PQ KEM in COSE

- PQ-KEM in a single recipient setup
- PQ-KEM in a multiple recipient setup

Single Recipient / One Layer Structure



- The plaintext will be encrypted using the CEK. The resulting ciphertext is either included in the COSE_Encrypt0 or is detached.

Multiple Recipients / Two Layer Structure

- Layer 0 contains the content (plaintext) encrypted with the CEK.
- Layer 1 (corresponding to a recipient structure) contains parameters needed for PQ-KEM to generate a shared secret used to encrypt the CEK.
  - The output ('ct') from the PQ KEM Encaps algorithm in the 'encapsulated_key' header parameter
  - The encrypted CEK in the encCEK structure.

Next Steps

- Consider for WG adoption
- Comments and suggestions are welcome