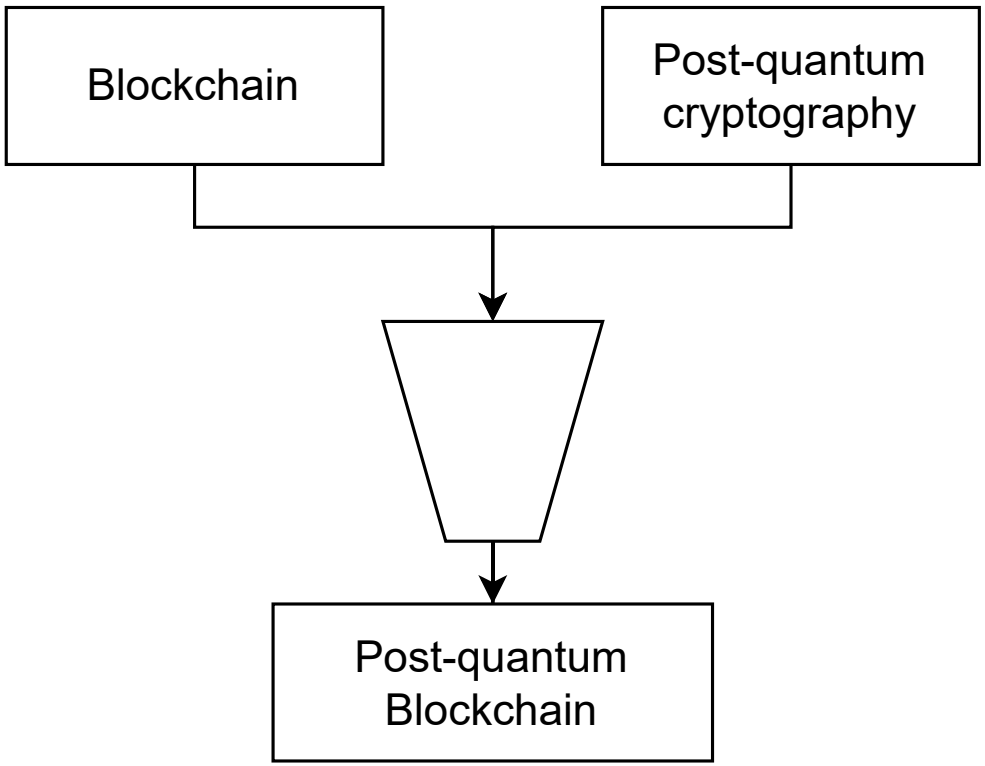
Blockchain Resistant to Quantum Attack

Michal Ľaš

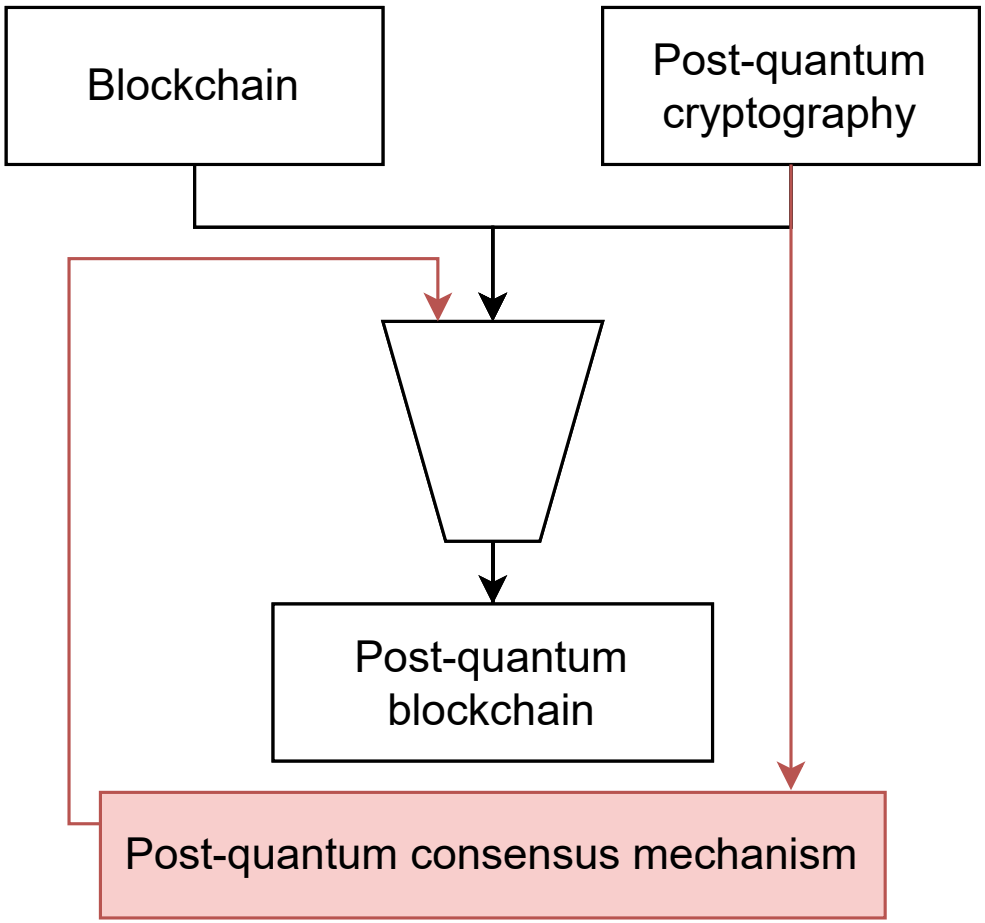
Supervisor: Mgr. Kamil Malinka, Ph.D.

11.06.2024

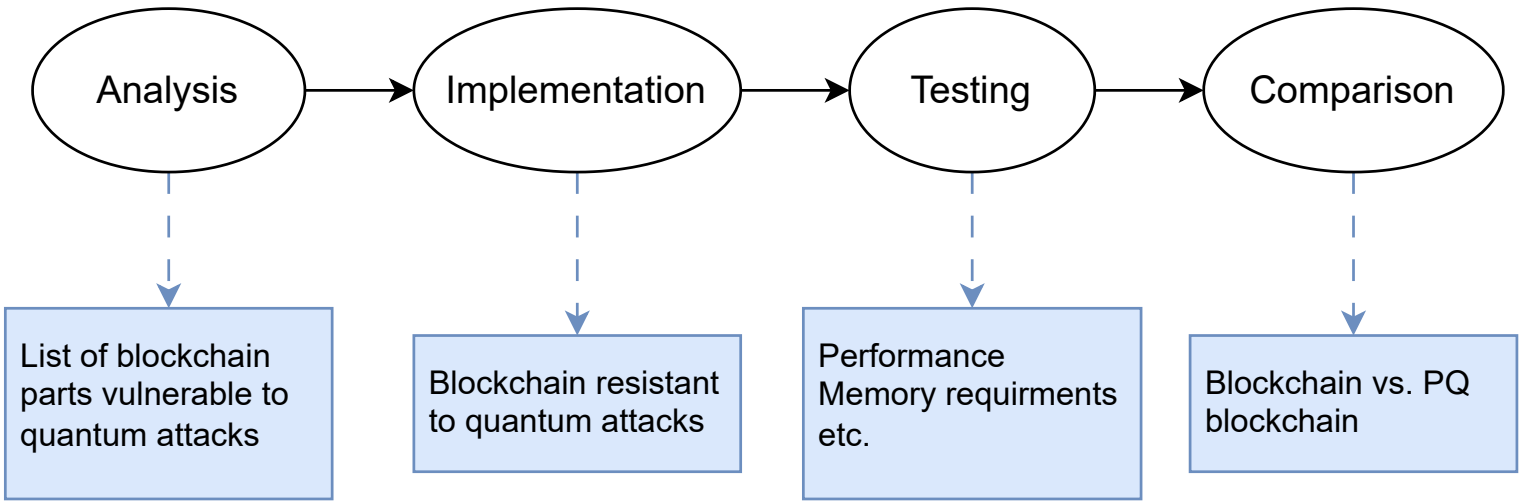
Motivation


Blockchain
Post-quantum cryptography
Post-quantum Blockchain

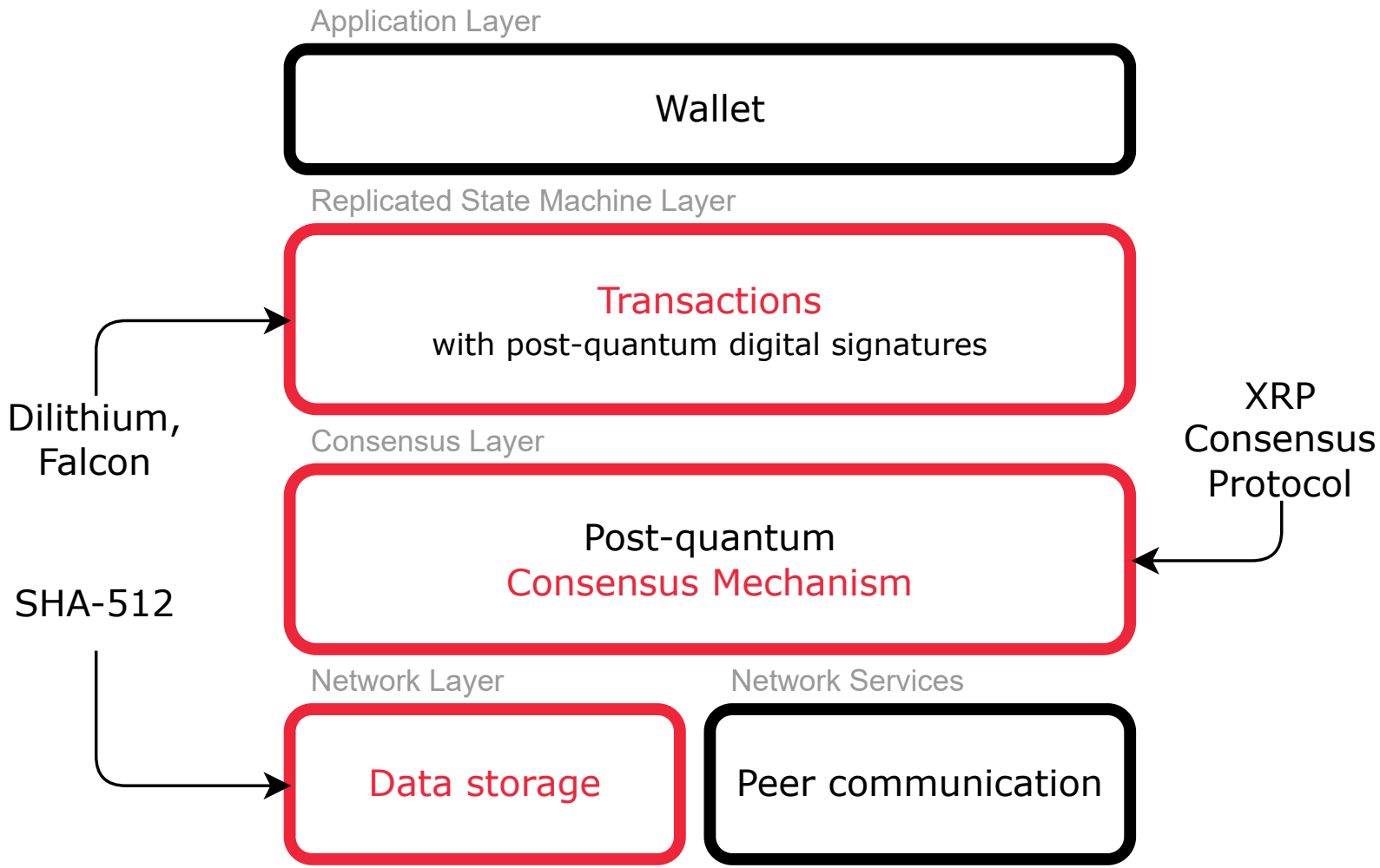
Motivation


Blockchain
Post-quantum cryptography
Post-quantum blockchain
Post-quantum consensus mechanism

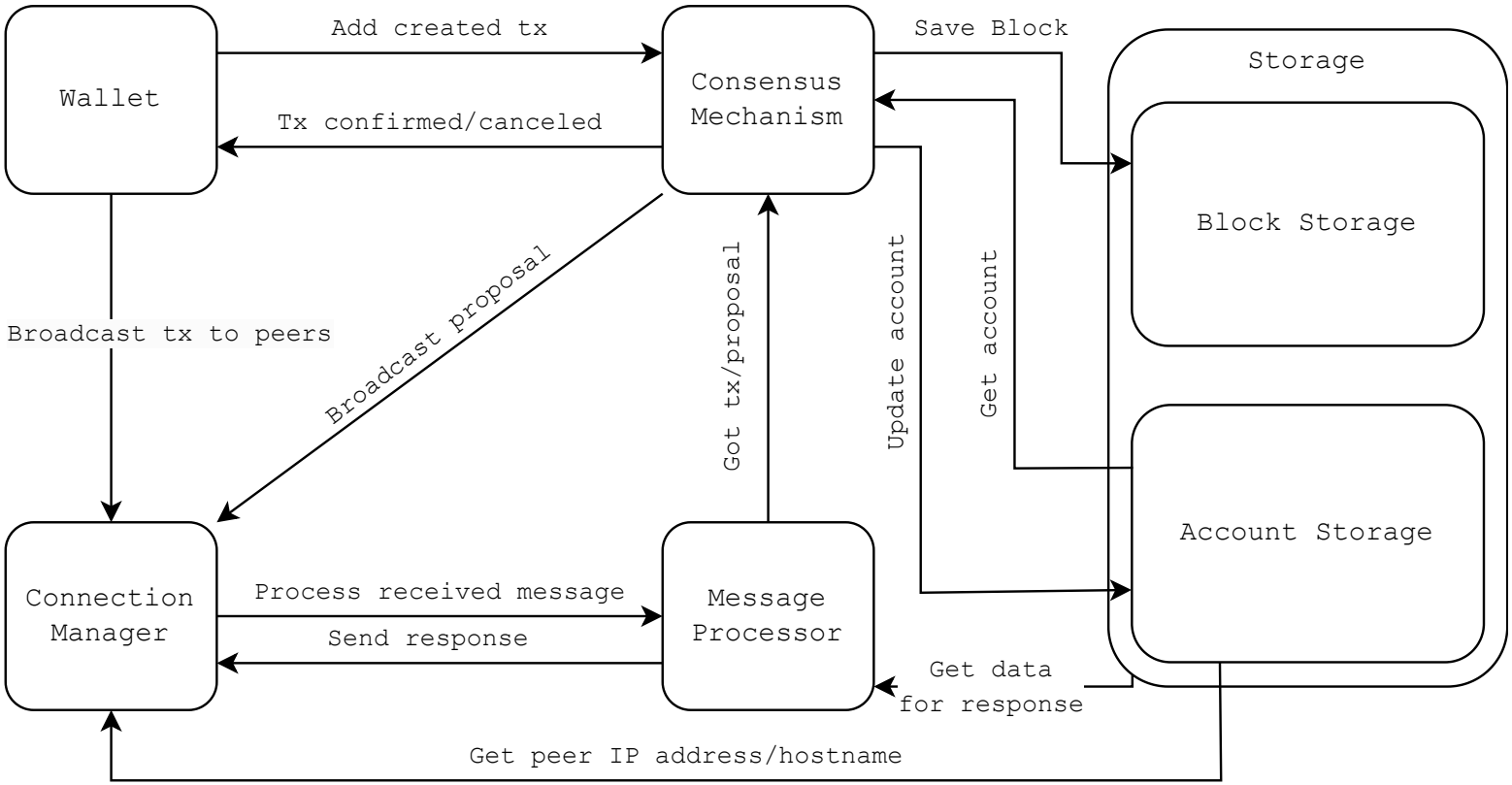
Objectives of the Thesis

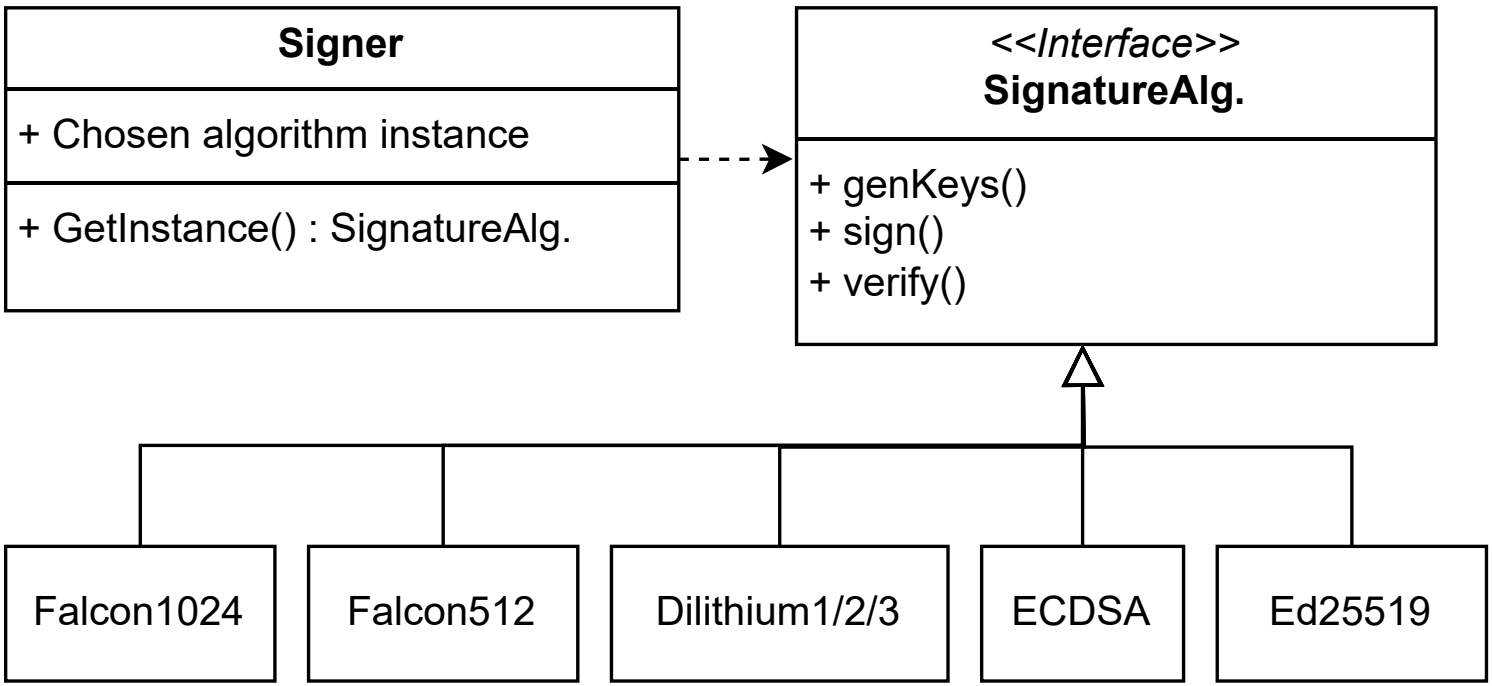


Vulnerable blockchain parts

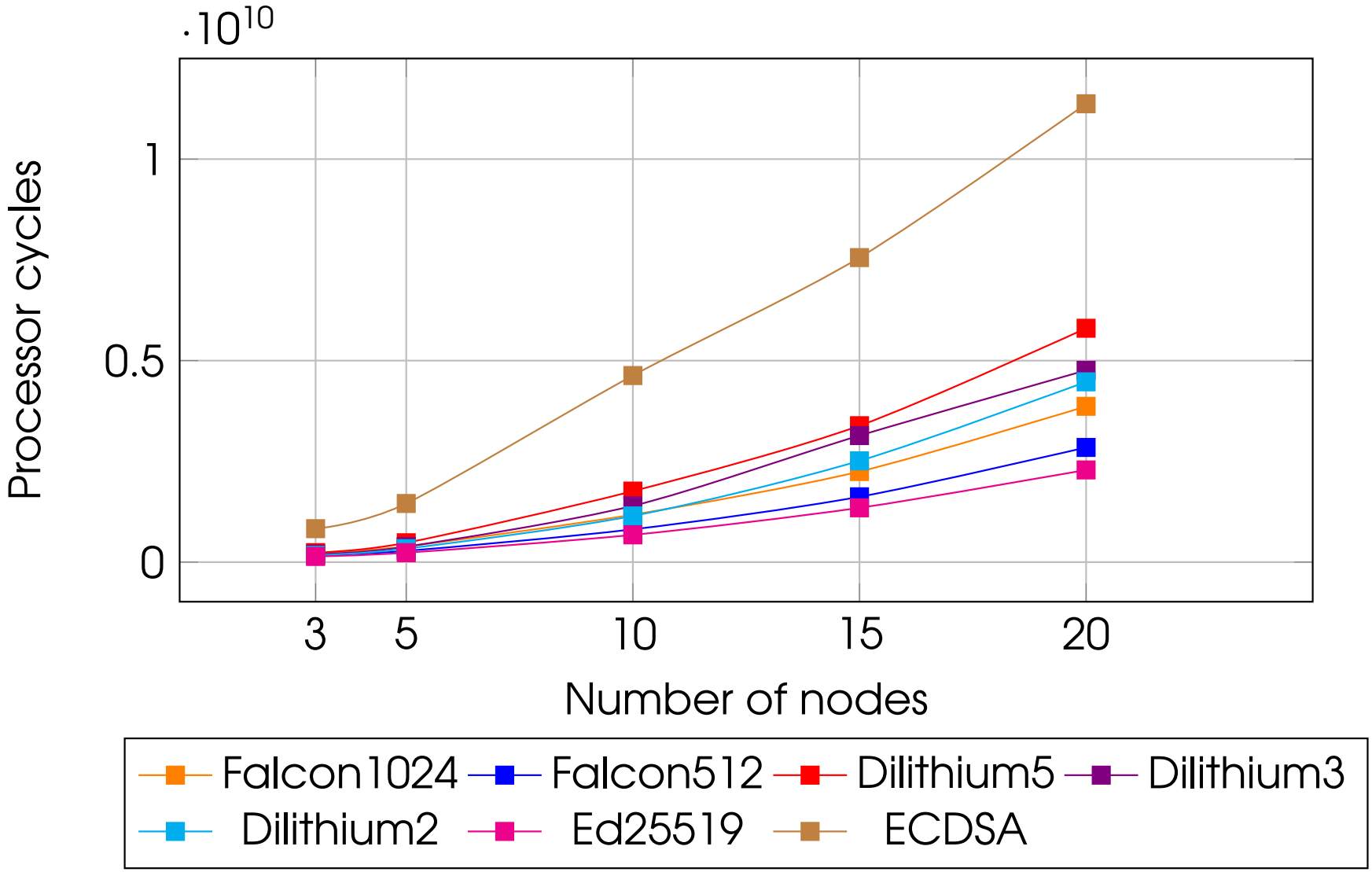


Node design

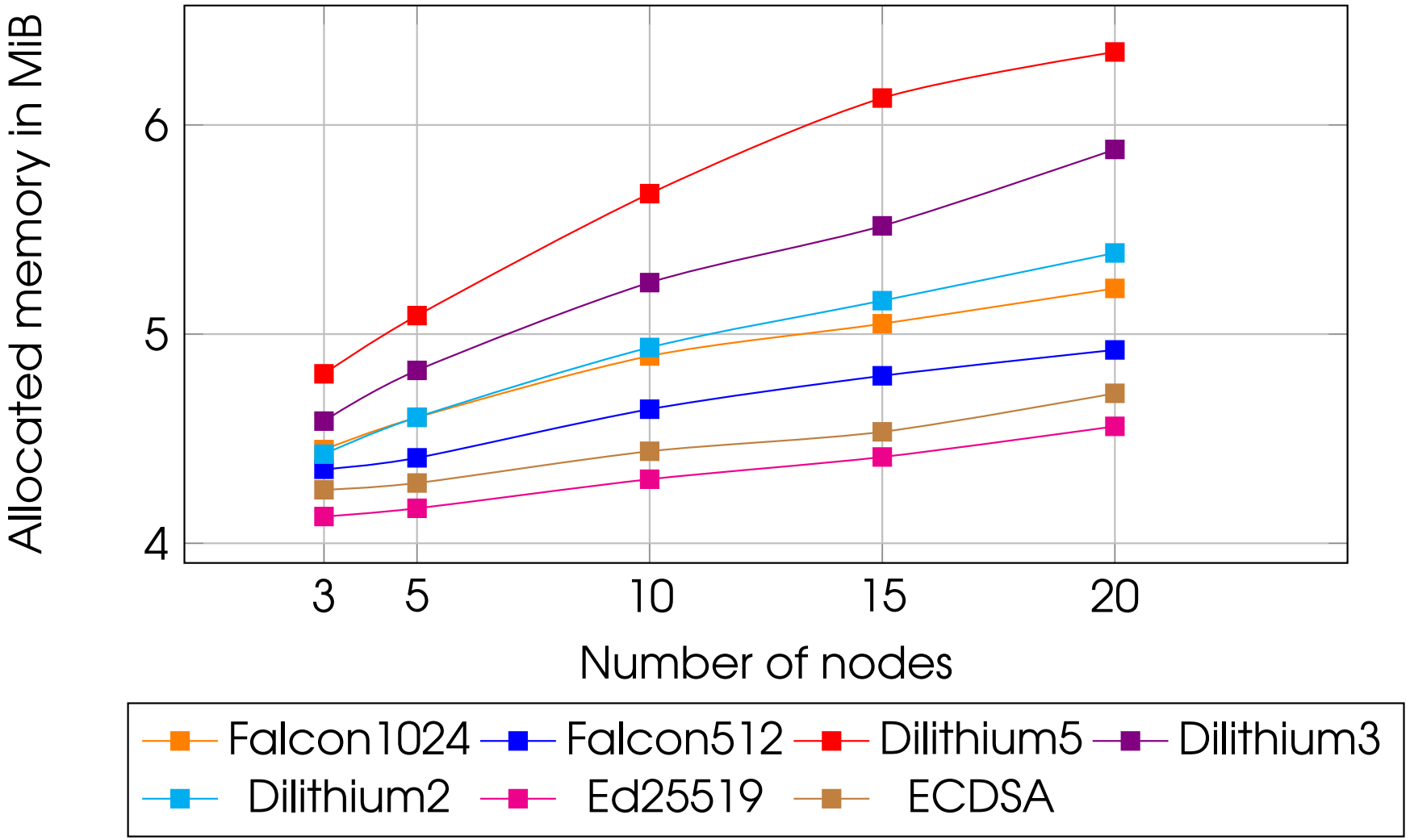

Wallet
Add created tx
Tx confirmed/canceled
Consensus Mechanism
Save Block
Storage
Block Storage
Account Storage
Broadcast tx to peers
Broadcast proposal
Got tx/proposal
Update account
Get account
Connection Manager
Process received message
Send response
Message Processor
Get data for response
Get peer IP address/hostname


Signer
+ Chosen algorithm instance
+ GetInstance() : SignatureAlg.
<<Interface>>
SignatureAlg.
+ genKeys()
+ sign()
+ verify()
Falcon1024
Falcon512
Dilithium1/2/3
ECDSA
Ed25519

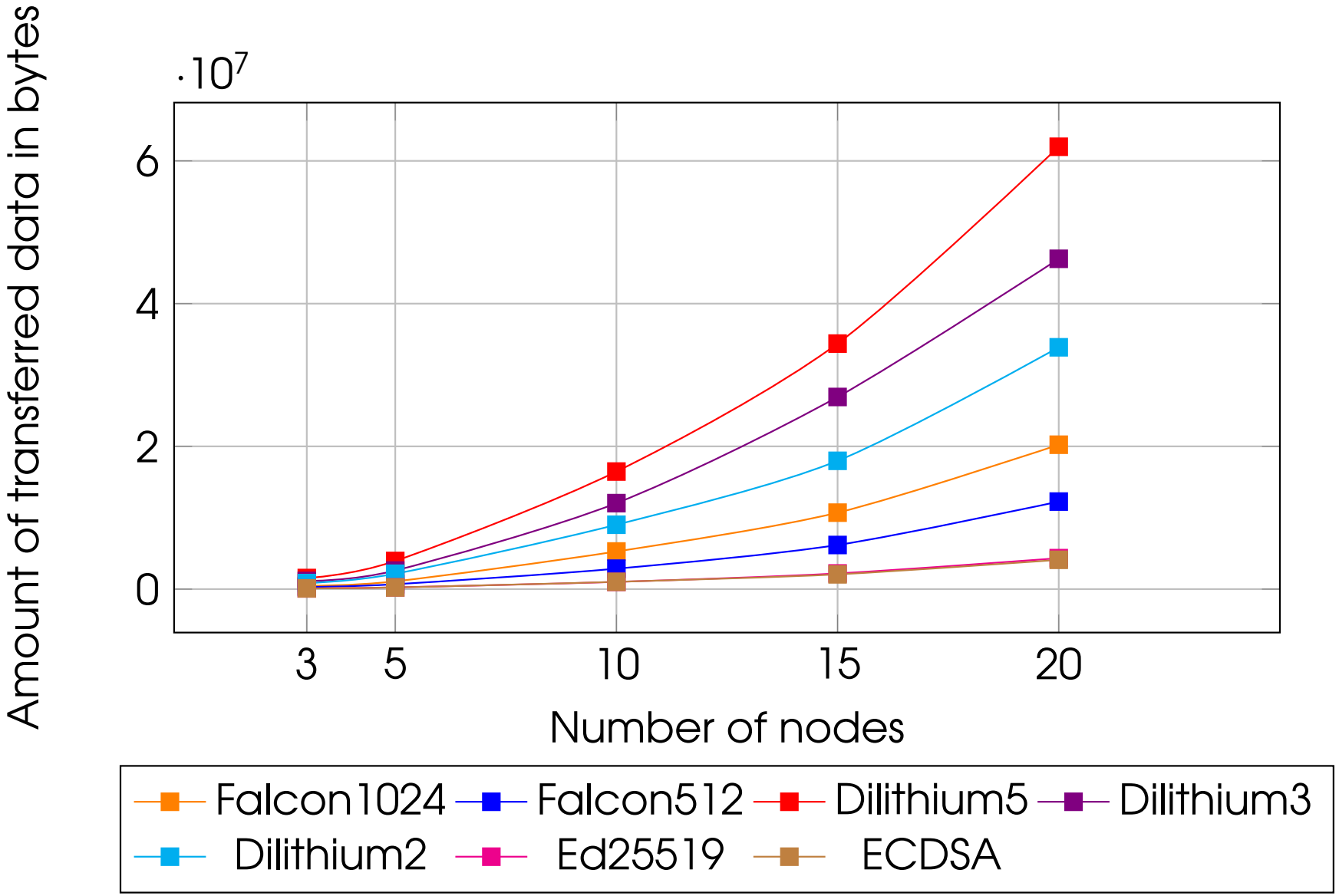
Performance



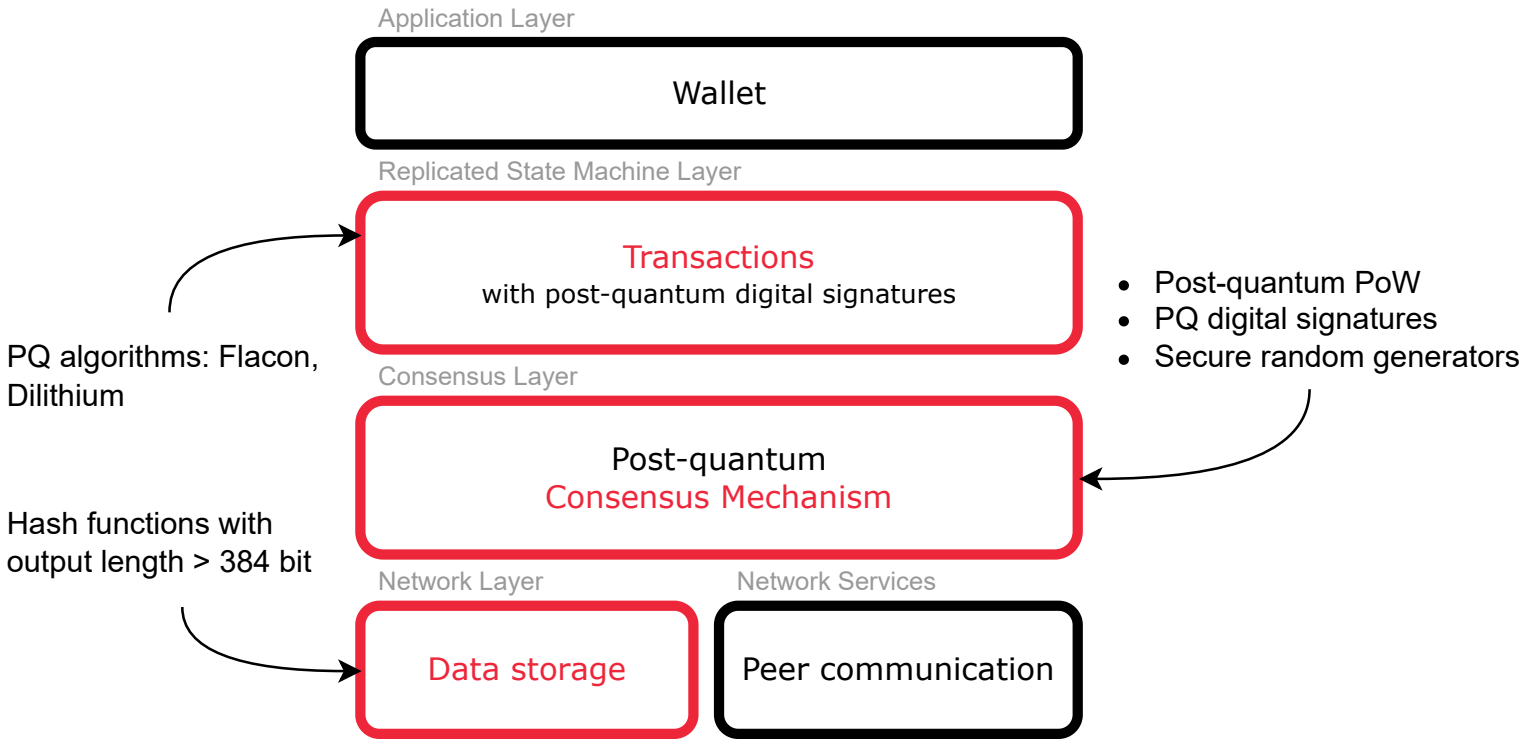
Memory requirments



Transferred data



Thank You for Your Attention!



Opponent's Questions

Ako ovplyvňuje samotná implementácia postkvantových kryptografických algoritmov celkovú veľkosť a účinnosť blockchainu? Ako by ste riešili potenciálne kompromisy z hľadiska väčšej veľkosti a väčších výpočtových požiadaviek v akejkoľvek reálne nasadenej platforme blockchainu?

$$\Sigma = B \times (H + C \times T)$$

- Σ – celková veľkosť blockchainu
- B – počet blokov
- H – veľkosť hlavičky bloku
- C – počet transackcii
- T – veľkosť transakcie

Opponent's Questions

Dajú sa postkvantové algoritmy použiť aj na generovanie distribuovanej náhodnosti, ktorá je dôležitá napr. v konsenzuálnych protokoloch Proof-of-Stake blockchainoch? Ako by ste to riešili? (1,2); 1) ZKBdf: A ZKBoo-Based Quantum-Secure Verifiable Delay Function with Prover-Secret 2) Lattice-Based Proof-of-Work for Post-Quantum Blockchains

Účastníci blockchainu môžu spoločne prispievať k náhodnému výstupu vypočítaním VDF.

ZKBdf

- Post-kvantovú odolnosť zaručuje nulová znalosť – kvantový počítač nedokáže predikovať výsledky VDF ostatných účastníkov blockchainu.

Lattice-Based Proof-of-Work

- Post-kvantovú odolnosť zaručujú algoritmy založené na mriežkach.

Key and ciphertext sizes (in bytes) for the KEM algorithms

Algorithm	Claimed Security	Public key	Private k
KYBER512	Level 1	800	1632
KYBER768	Level 3	1 184	2 400
KYBER1024	Level 5	1 568	3 168
Classic McEliece348864	Level 1	261 120	6 492
Classic McEliece460896	Level 3	524 160	13 608
Classic McEliece6688128	Level 5	104 992	13 932
Classic McEliece6960119	Level 5	1 047 319	13 948
Classic McEliece8192128	Level 5	1 357 824	14 120
HQC-128	Level 1	2 249	40
HQC-192	Level 3	4 522	40
HQC-256	Level 5	7 245	40

Key and signature sizes (in bytes) for the digital signatures algorithms

Algorithm	Claimed Security	Public key	Private key	Signa
Dilithium	Level 2	1 312	2 528	2 42
	Level 3	1 952	4 000	3 29
	Level 5	2 592	4 864	4 59
FALCON-512	Level 1	897	7 553	66
FALCON-1024	Level 5	1 793	13 953	1 28
SPHINCS$^+$-128s	Level 1	32	64	7 85
SPHINCS$^+$-128f	Level 1	32	64	17 0
SPHINCS$^+$-192s	Level 3	48	96	16 2
SPHINCS$^+$-192f	Level 3	48	96	35 6
SPHINCS$^+$-256s	Level 5	64	128	29 7
SPHINCS$^+$-256f	Level 5	64	128	49 8

Performance of KEM algorithms (in processor cycles)

Algorithm	Keygen	Encapsulation	Decapsula
KYBER512	29 172	36 768	26 943
KYBER768	45 407	54 332	42 098
KYBER1024	61 960	74 939	60 053
Classic McEliece348864	151 761 145	47 503	119 873
Classic McEliece460896	385 383 414	90 694	231 764
Classic McEliece6688128	591 004 800	191 851	273 034
Classic McEliece6960119	567 788 742	164 539	251 788
Classic McEliece8192128	625 667 532	203 624	268 867
HQC-128	104 115	197 030	360 575
HQC-192	244 636	459 309	766 797
HQC-256	447 179	845 083	1 425 97

Performance of signature algorithms (in processor cycles)

Algorithm	Keygen	Signing	Verifycation
Dilithium2	90 195	236 975	87 348
Dilithium3	153 215	380 755	144 980
Dilithium5	247 152	476 989	236 726
FALCON-512	21 234 790	888 844	143 976
FALCON-1024	63 158 867	1 800 943	292 065
SPHINCS$^+$-128s	5 9910 564	447 597 974	745 416
SPHINCS$^+$-128f	933 692	21 966 943	1 891 461
SPHINCS$^+$-192s	96 144 674	1 080 729 340	1 152 859
SPHINCS$^+$-192f	1 405 335	38 270 621	2 709 479
SPHINCS$^+$-256s	59 723 455	786 789 398	1 565 715
SPHINCS$^+$-256f	3 740 593	79 046 495	2 729 293