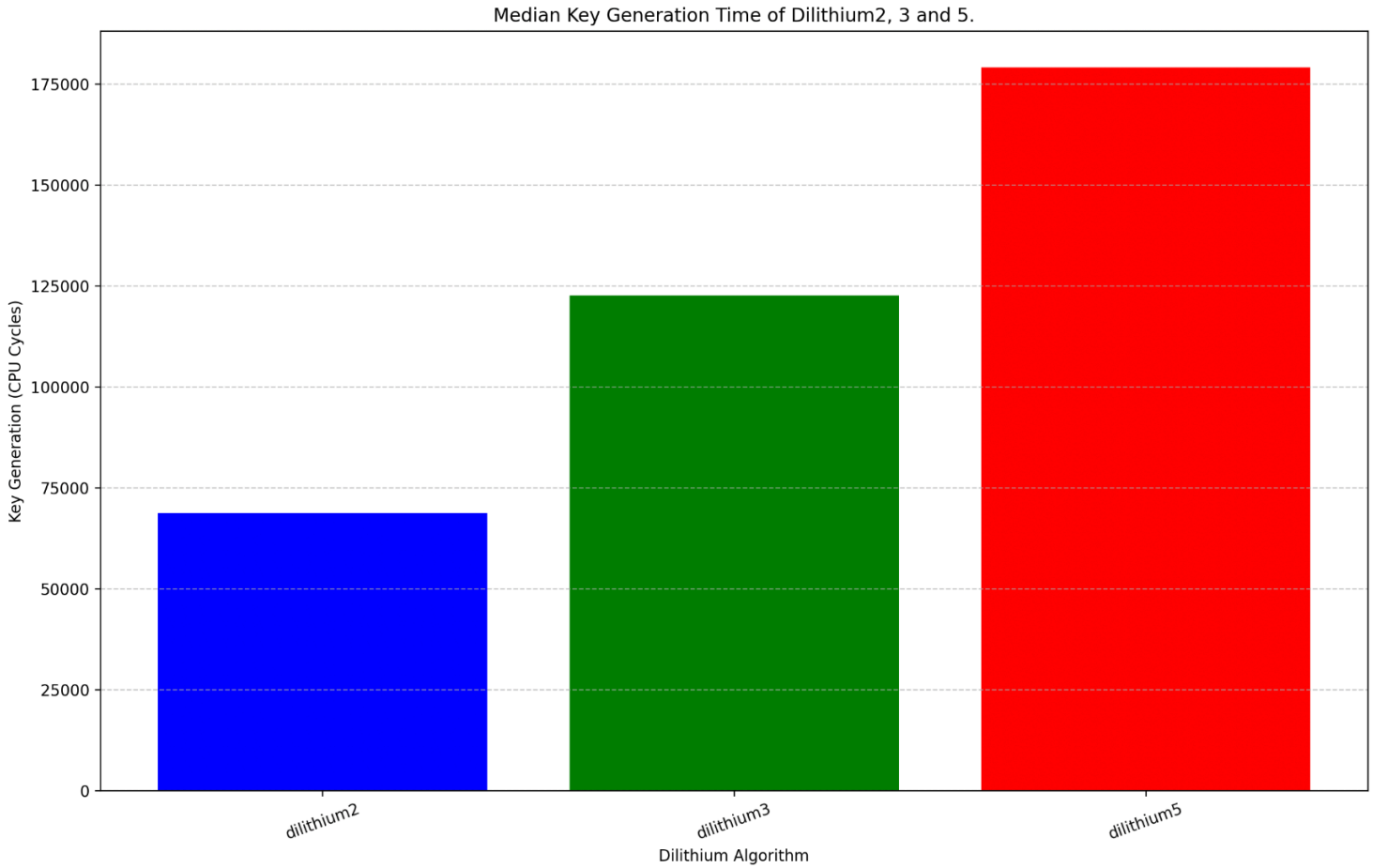
Digital Signature Post-Quantum Algorithms Performance

Dilithium

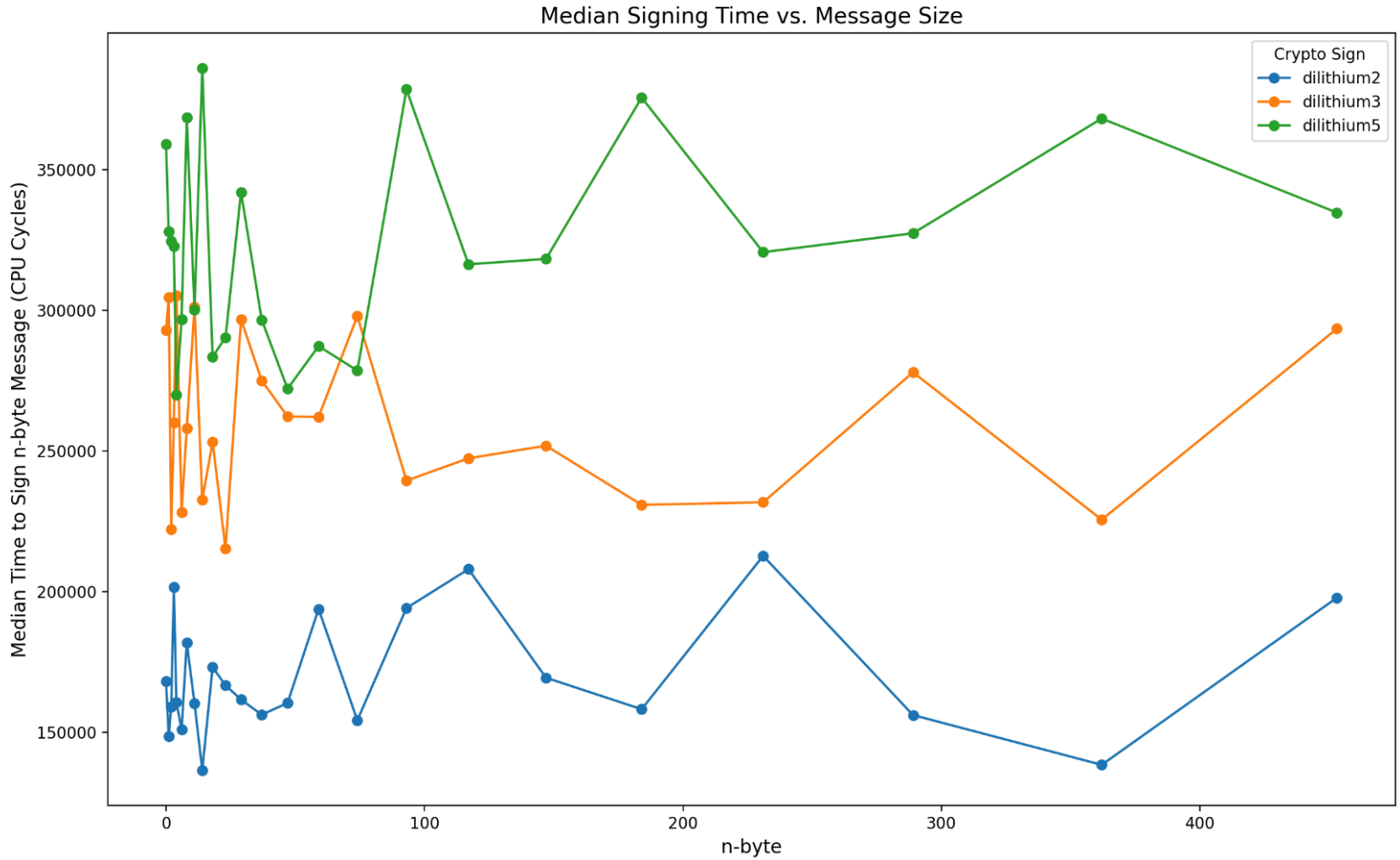
Dilithium Key Generation

Median Time (cycles) to generate a key pair: a secret key and a corresponding public key.



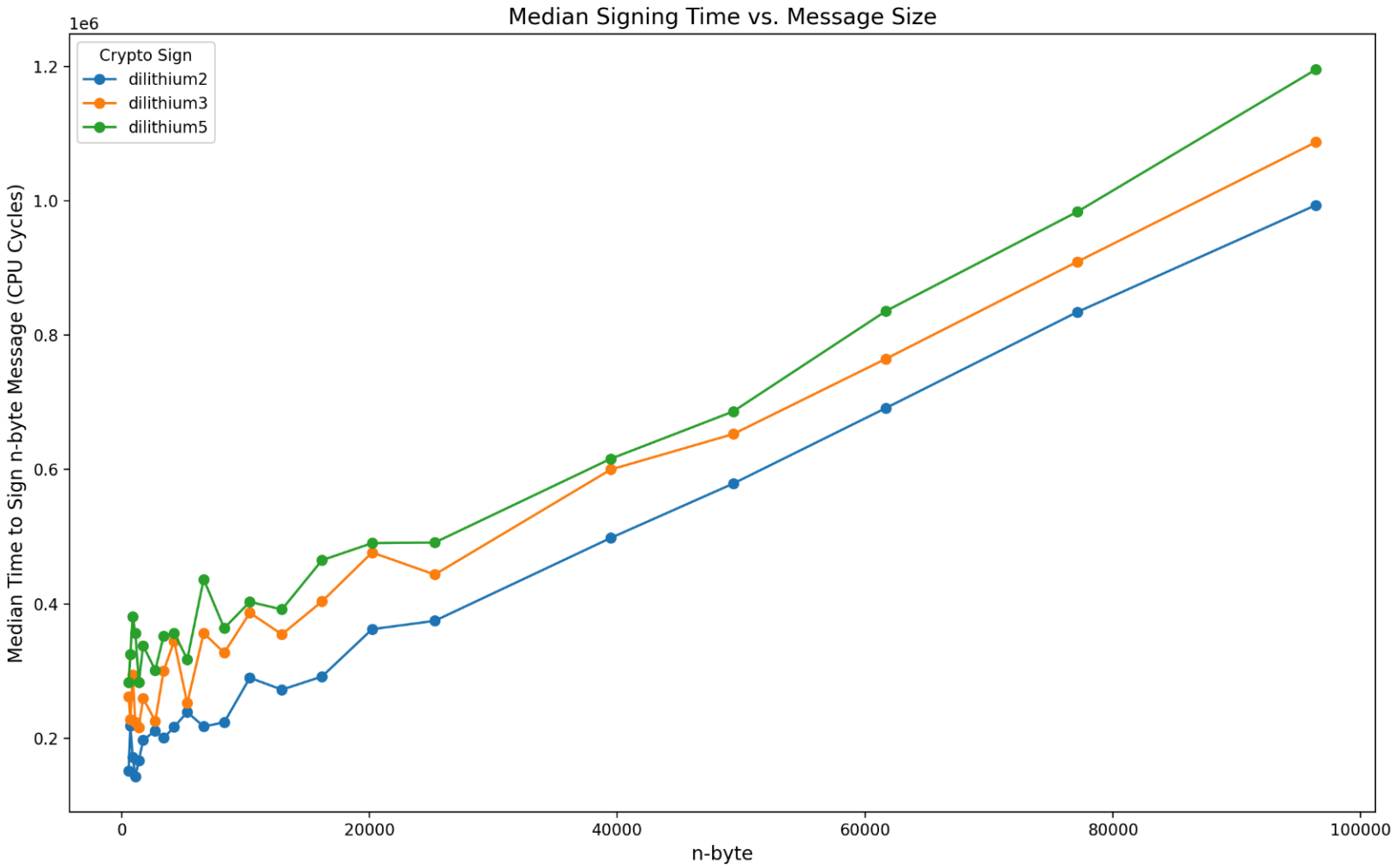
Dilithium Signing Time - 0-byte ≤ Messages ≤ 453-bytes

Time (Cycles) to sign a 0-byte ≤ message ≤ 453-bytes



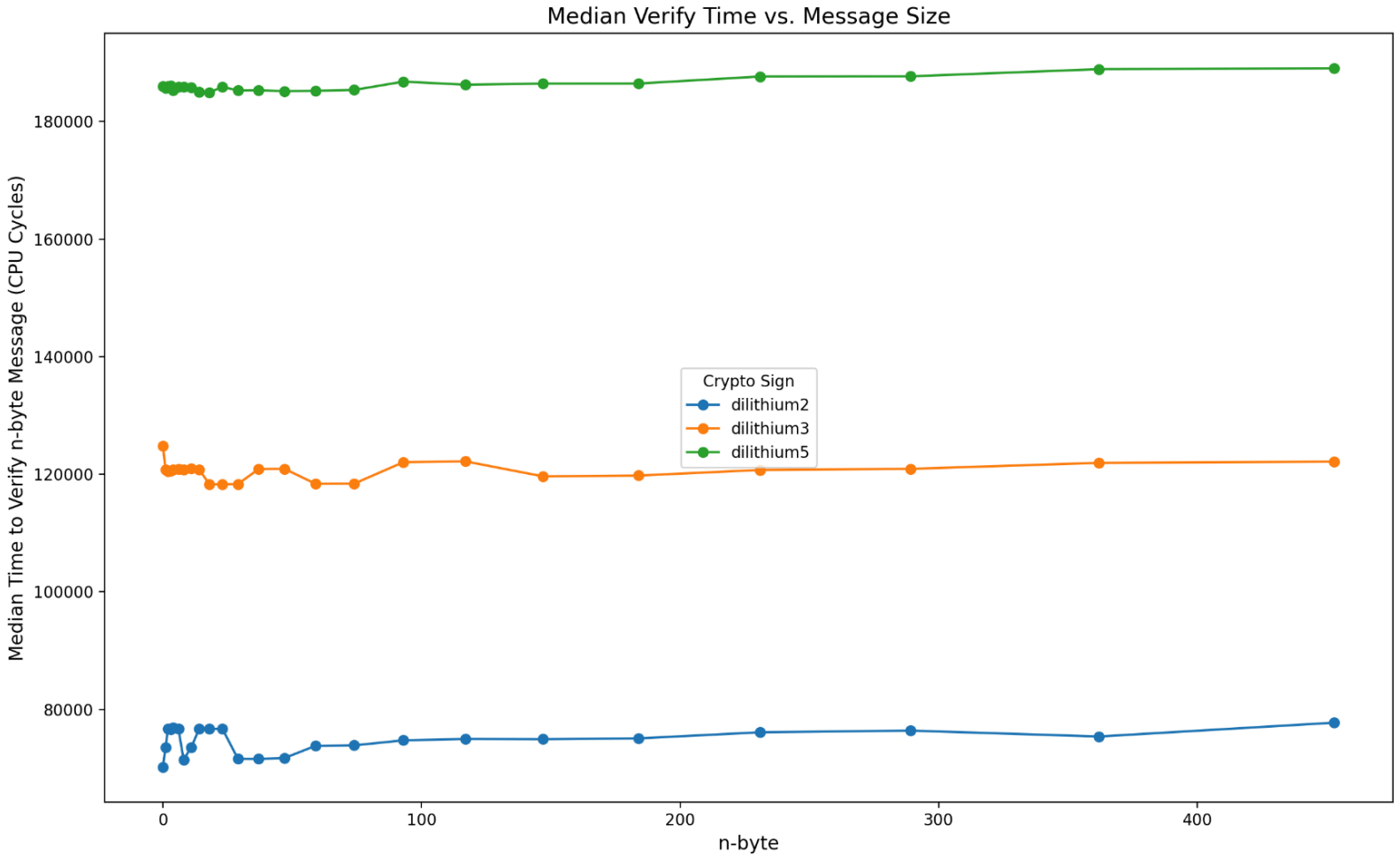
Dilithium Signing Time - 567-byte ≤ Messages ≤ 96397-byte

Time (Cycles) to sign a 567-byte ≤ message ≤ 96397-byte



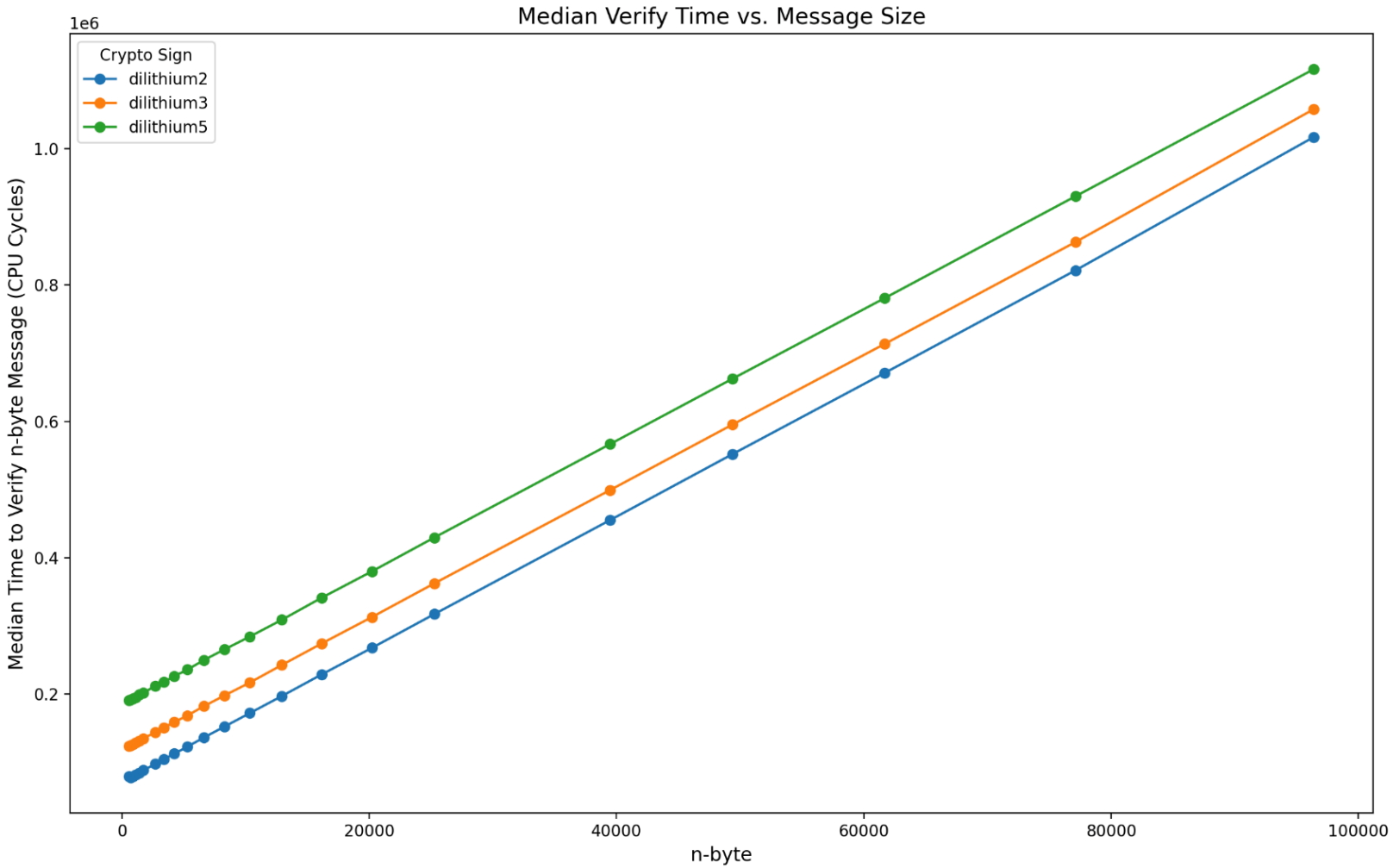
Dilithium Verifying Time - 0-byte ≤ Messages ≤ 453-bytes

Time (Cycles) to open a 0-byte ≤ message ≤ 453-bytes



Dilithium Verifying Time - 567-byte ≤ Messages ≤ 96397-byte

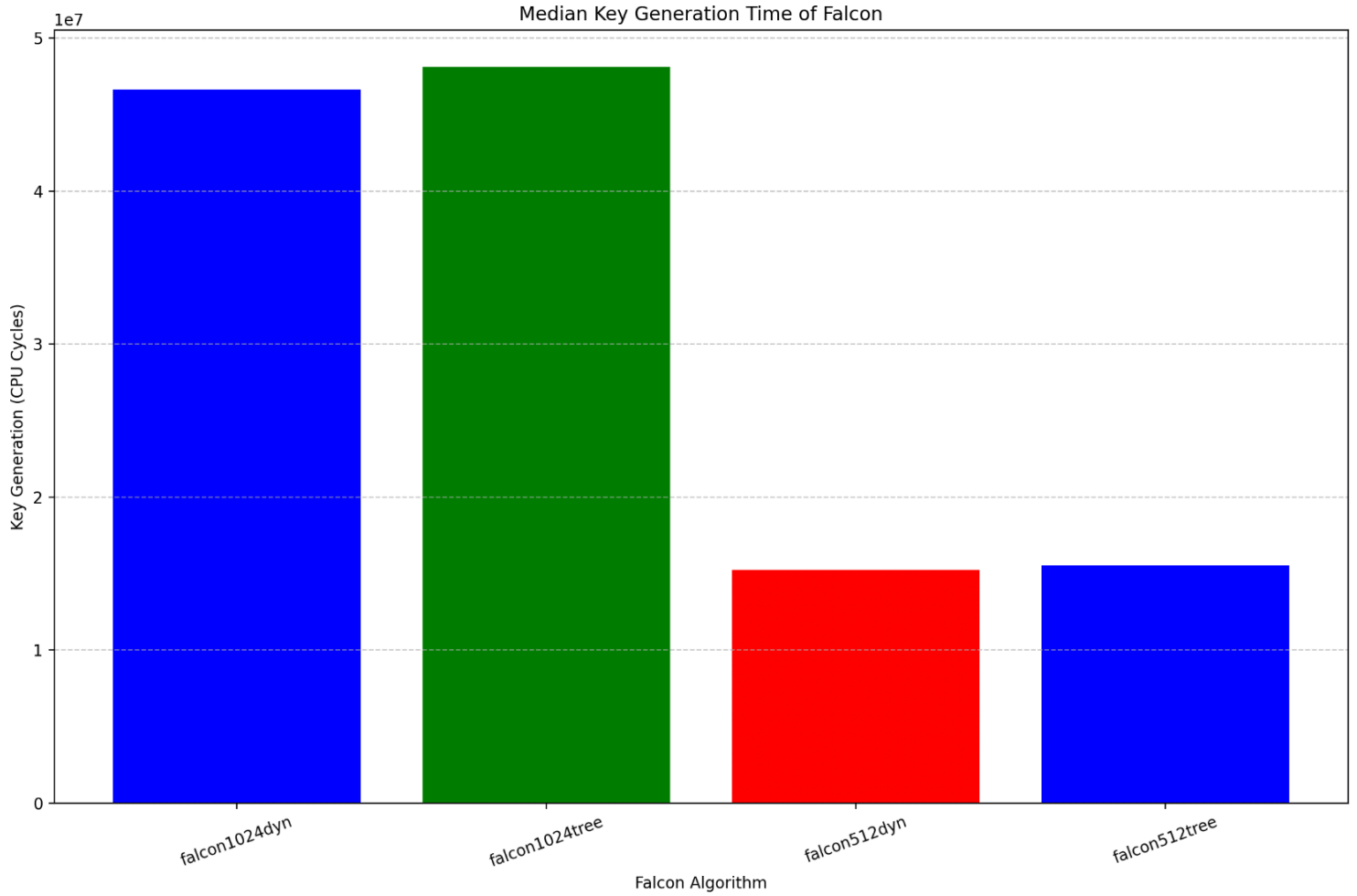
Time (Cycles) to open a 567-byte ≤ message ≤ 96397-byte



Falcon (Tree/Dyn)

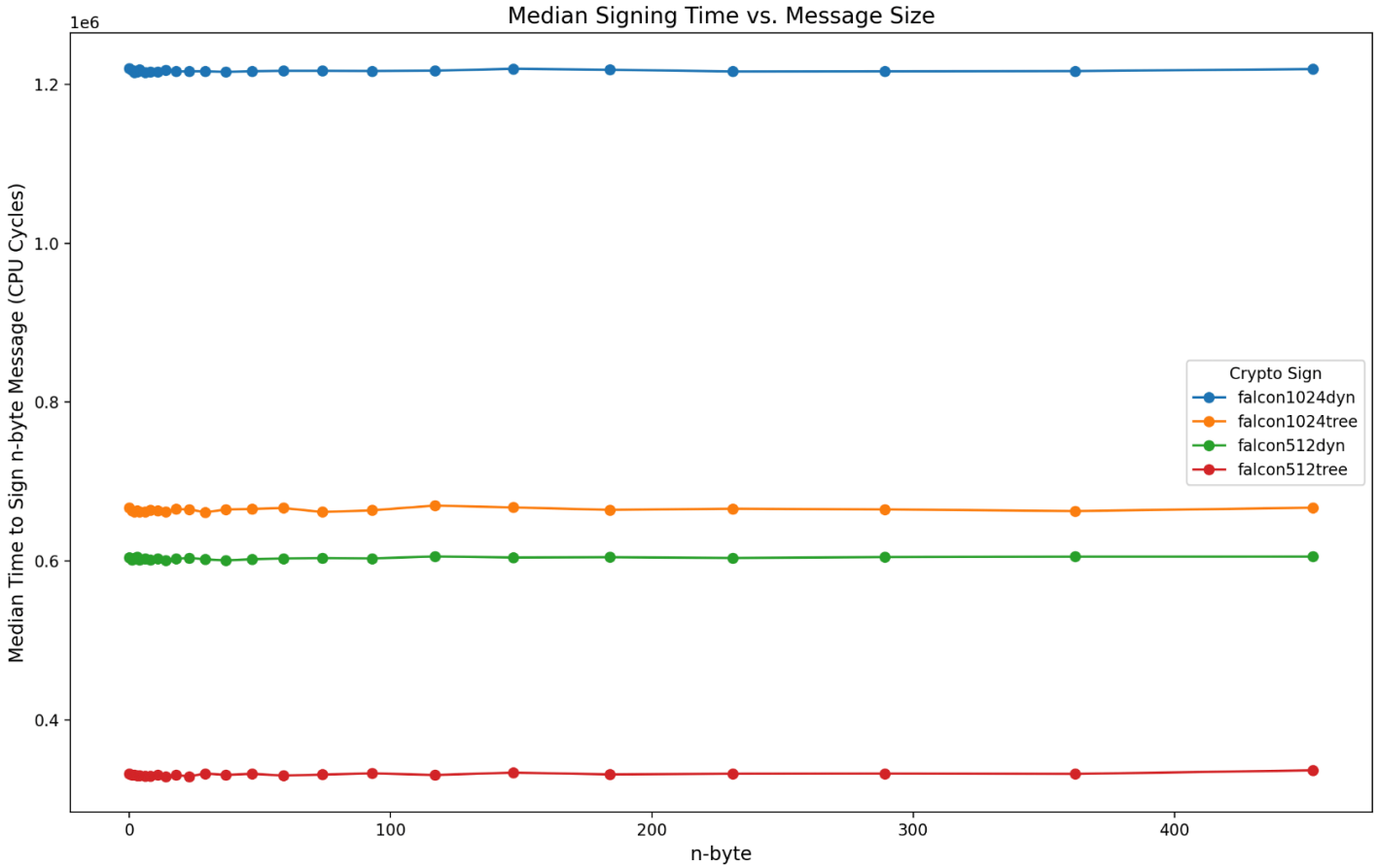
Falcon Key Generation

Median Time (cycles) to generate a key pair: a secret key and a corresponding public key.



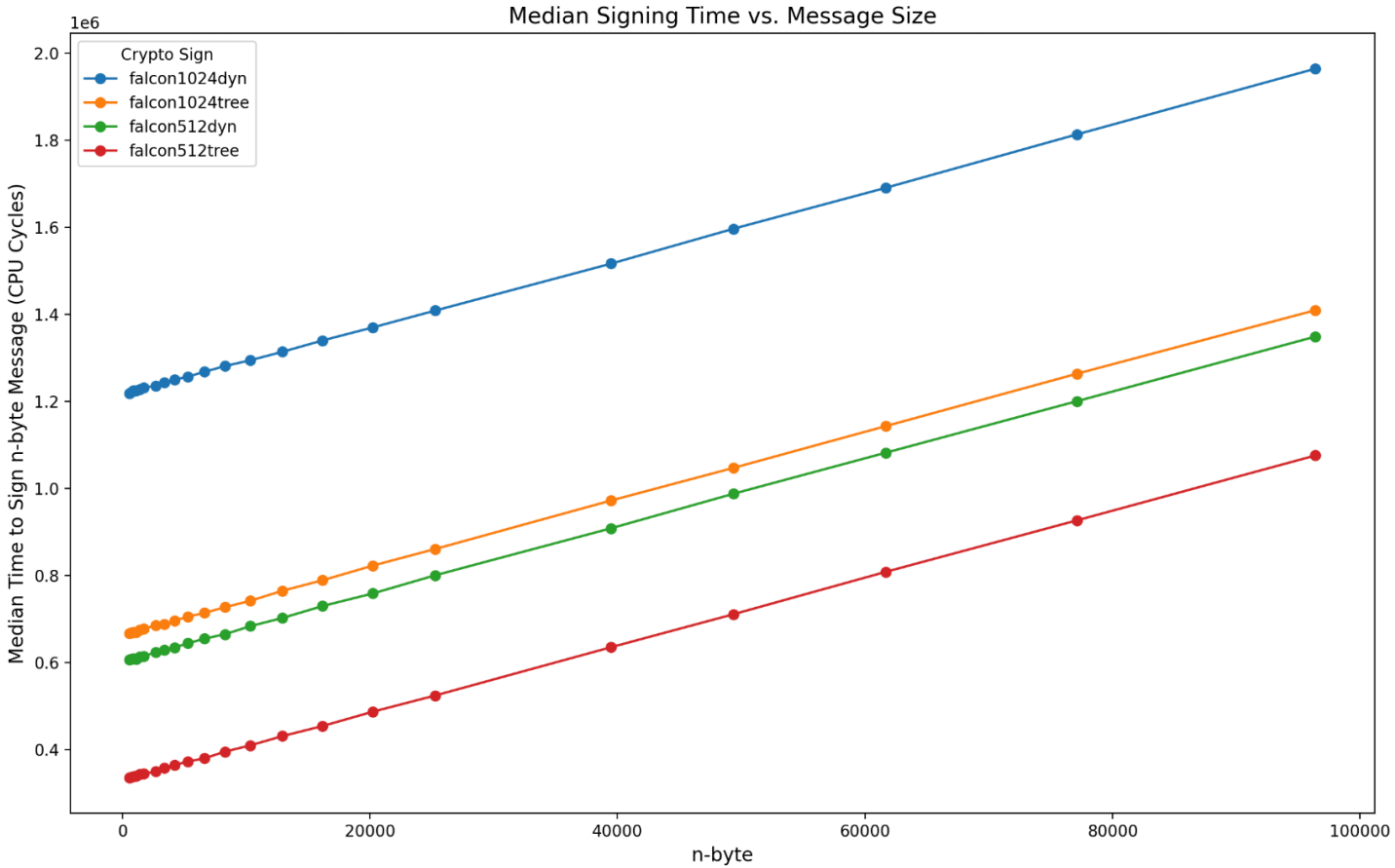
Falcon Signing Time - 0-byte ≤ Messages ≤ 453-bytes

Time (Cycles) to sign a 0-byte ≤ message ≤ 453-bytes



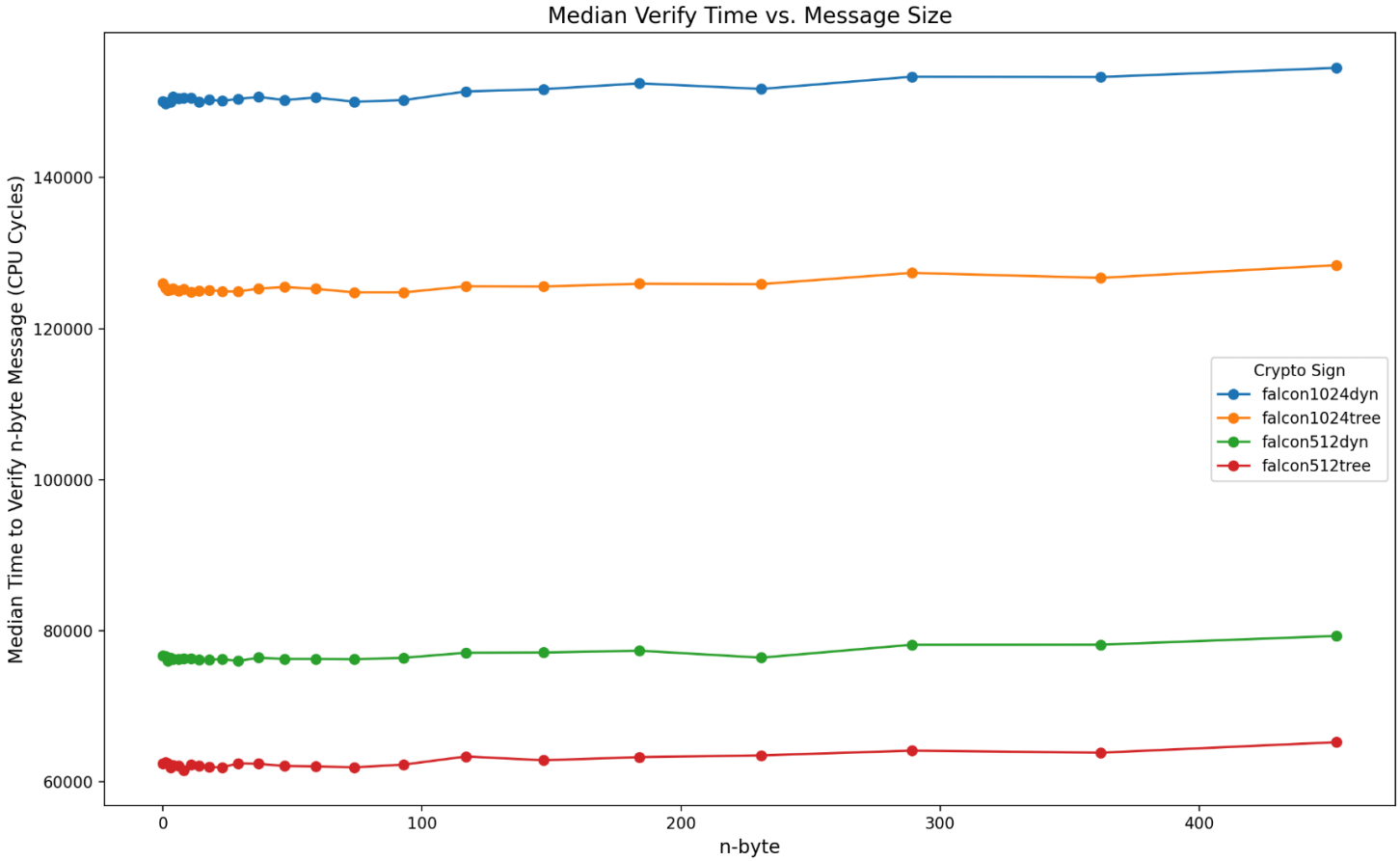
Falcon Signing Time - 567-byte ≤ Messages ≤ 96397-byte

Time (Cycles) to sign a 567-byte ≤ message ≤ 96397-byte



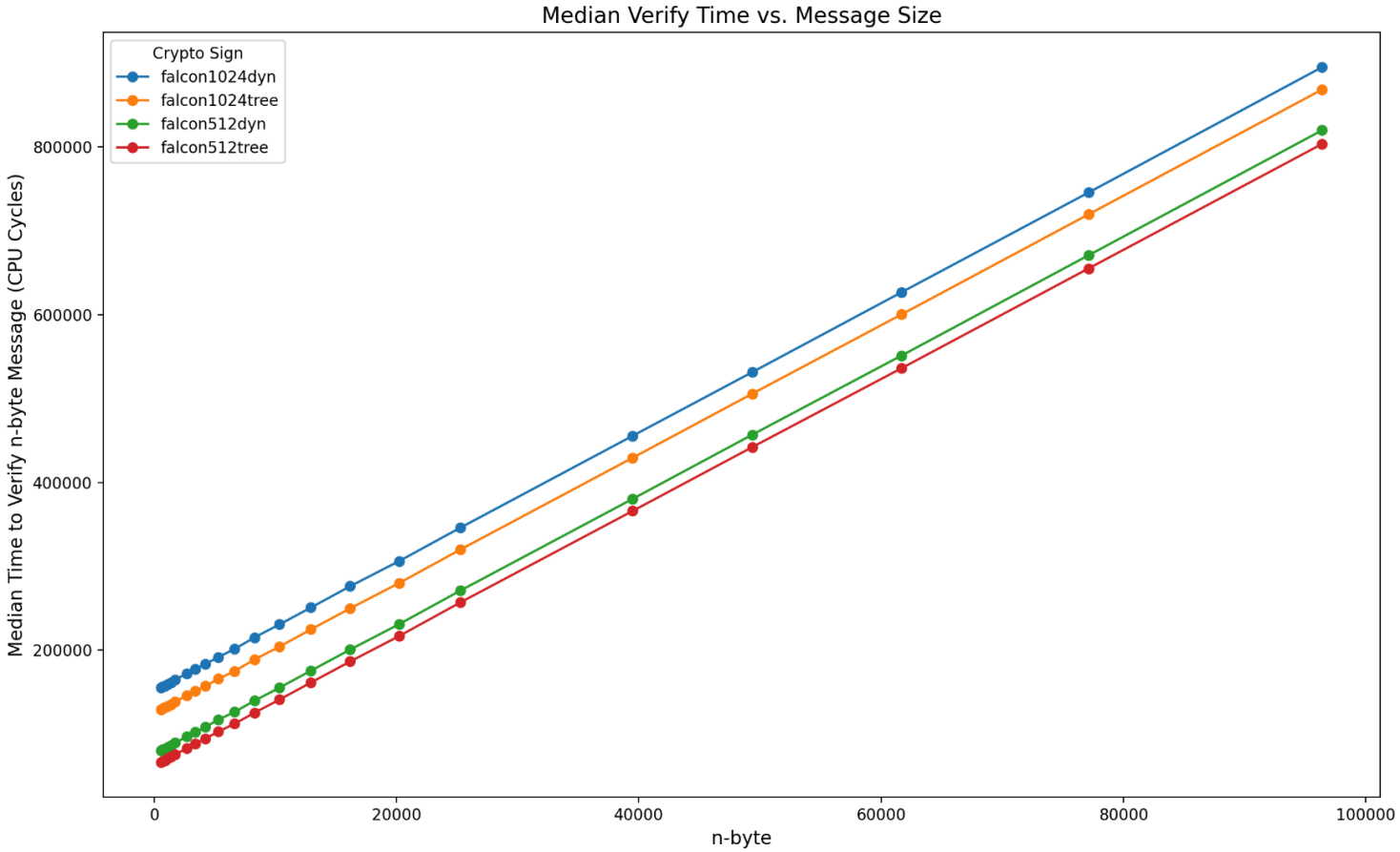
Falcon Verifying Time - 0-byte ≤ Messages ≤ 453-bytes

Time (Cycles) to open a 0-byte ≤ message ≤ 453-bytes



Falcon Verifying Time - 567-byte ≤ Messages ≤ 96397-byte

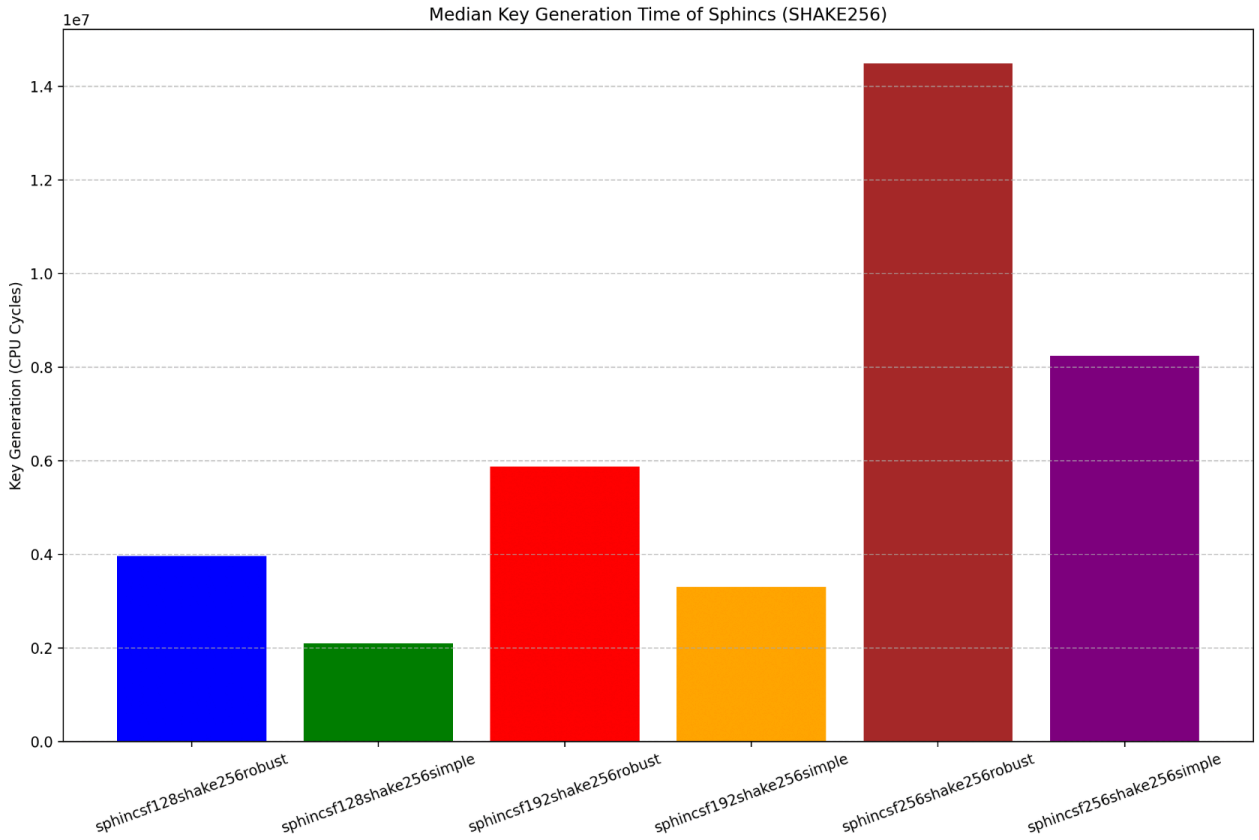
Time (Cycles) to open a 567-byte ≤ message ≤ 96397-byte



Sphincs-F (Shake256)

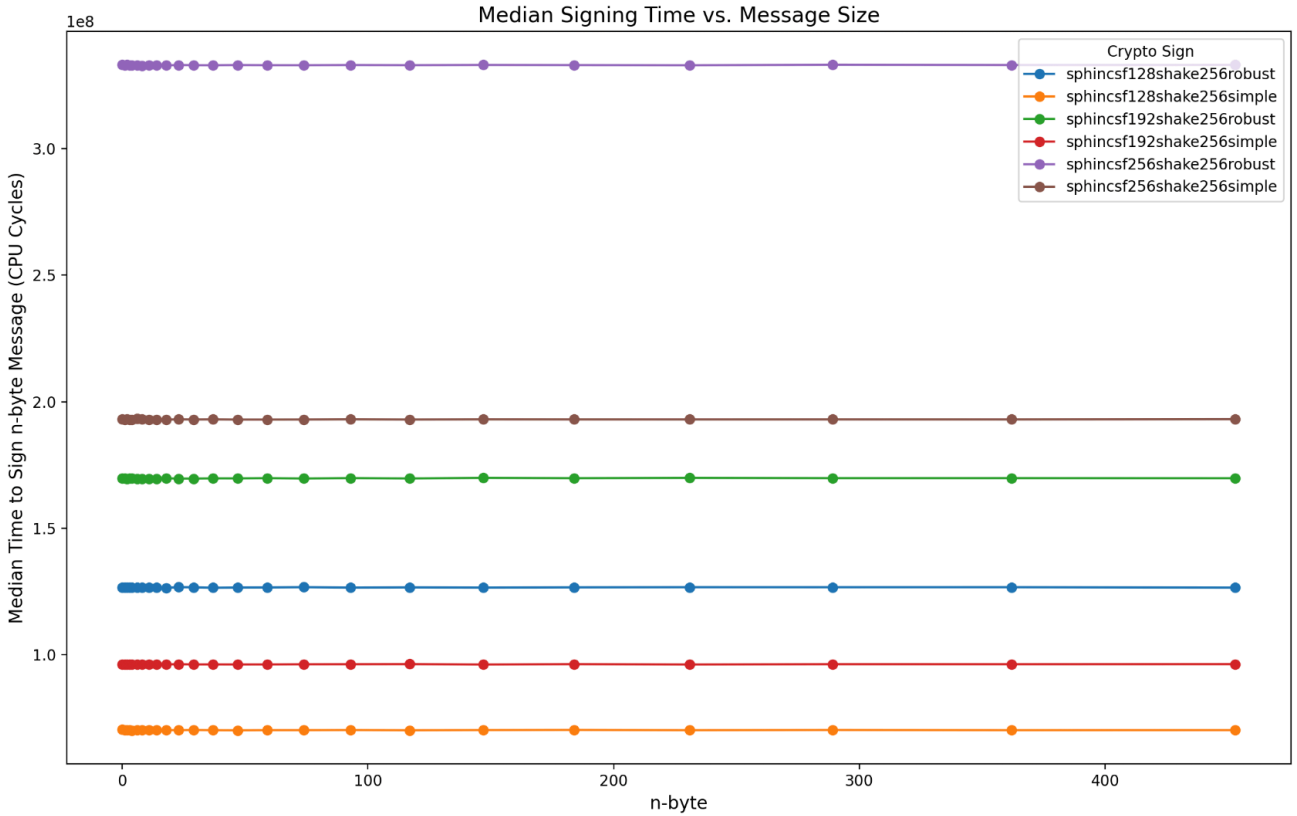
Sphincs-F (Shake256) Key Generation

Median Time (cycles) to generate a key pair: a secret key and a corresponding public key.



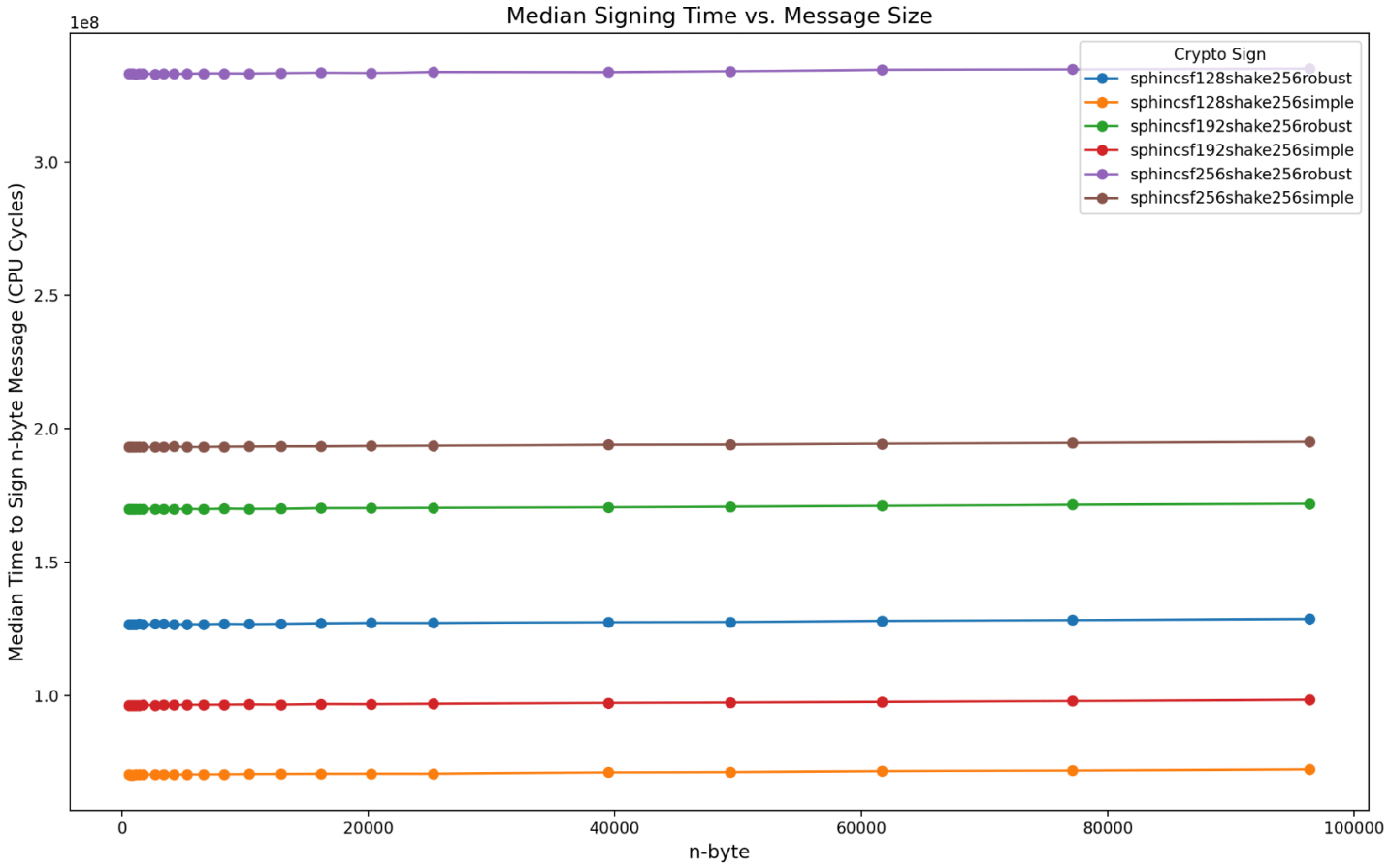
Sphincs-F (Shake256) Signing Time - 0-byte ≤ Messages ≤ 453-bytes

Time (Cycles) to sign a 0-byte ≤ message ≤ 453-bytes



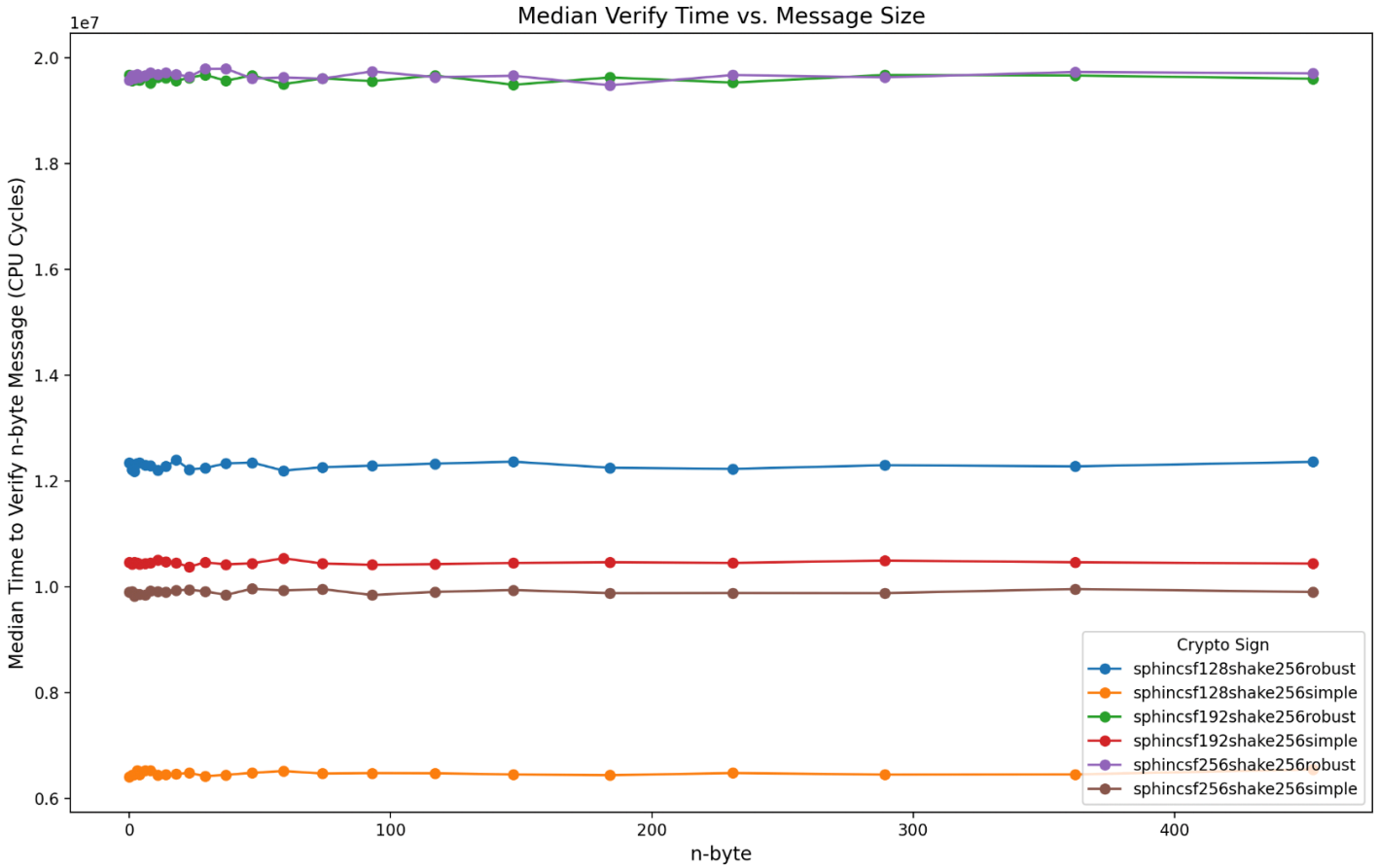
Sphincs-F (Shake256) Signing Time - 567-byte ≤ Messages ≤ 96397-byte

Time (Cycles) to sign a 567-byte ≤ message ≤ 96397-byte



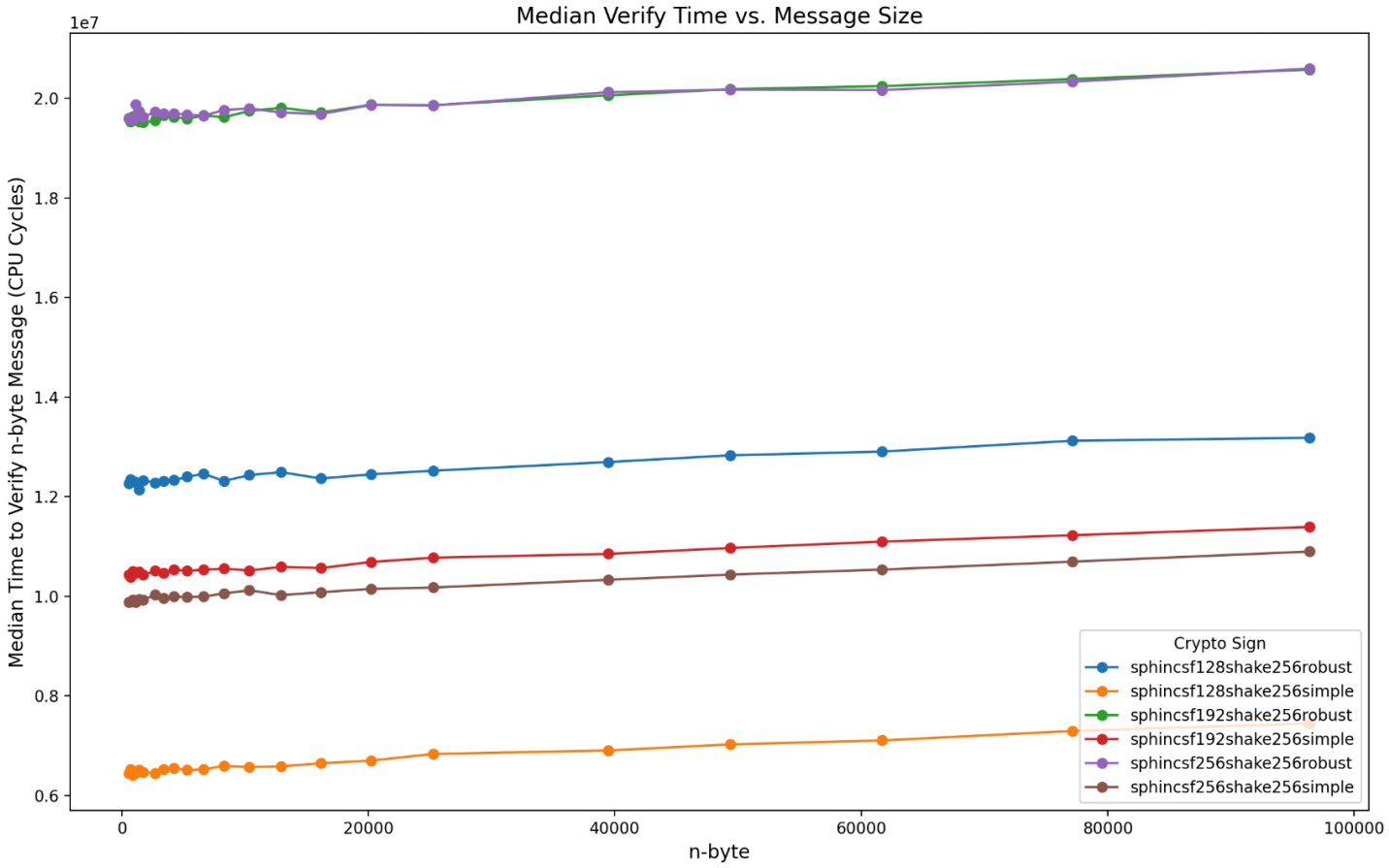
Sphincs-F (Shake256) Verifying Time - 0-byte ≤ Messages ≤ 453-bytes

Time (Cycles) to open a 0-byte ≤ message ≤ 453-bytes



Sphincs-F (Shake256) Verifying Time - 567-byte ≤ Messages ≤ 96397-byte

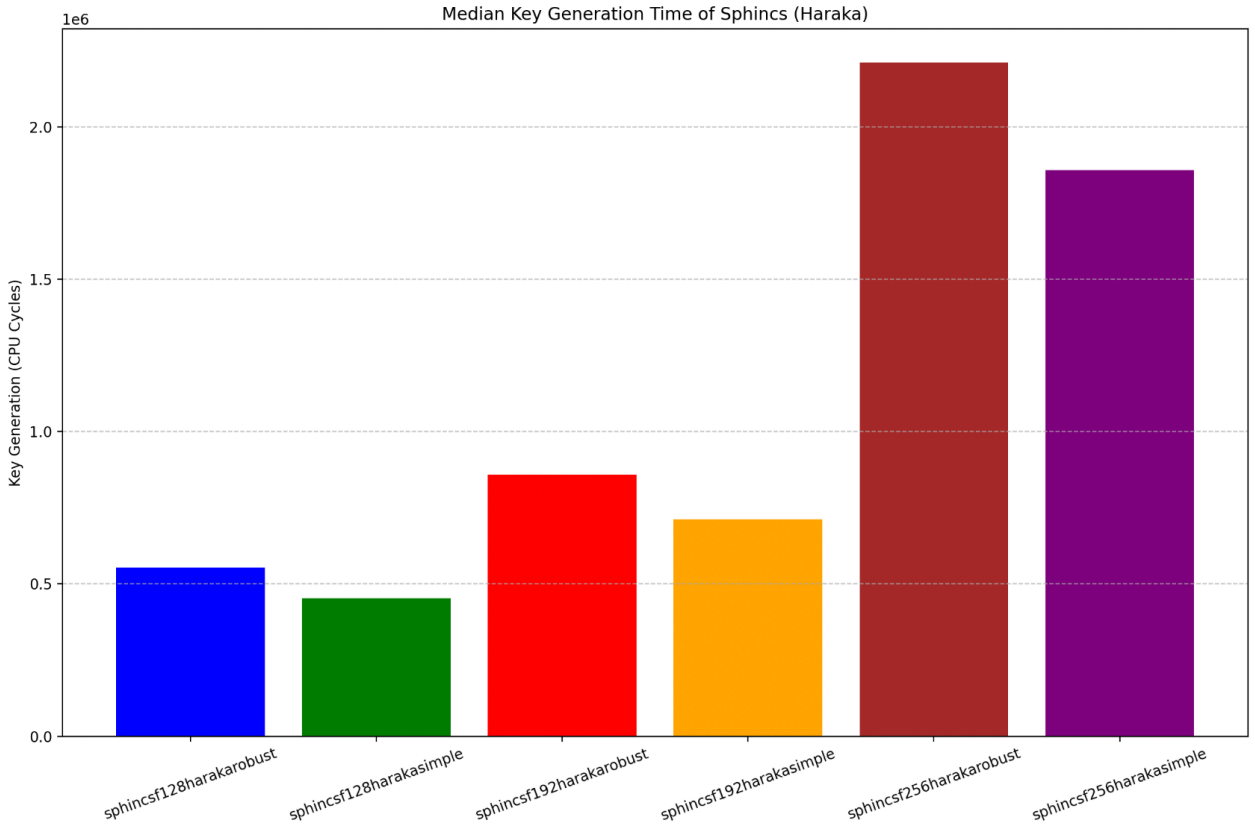
Time (Cycles) to open a 567-byte ≤ message ≤ 96397-byte



Sphincs-F (Haraka)

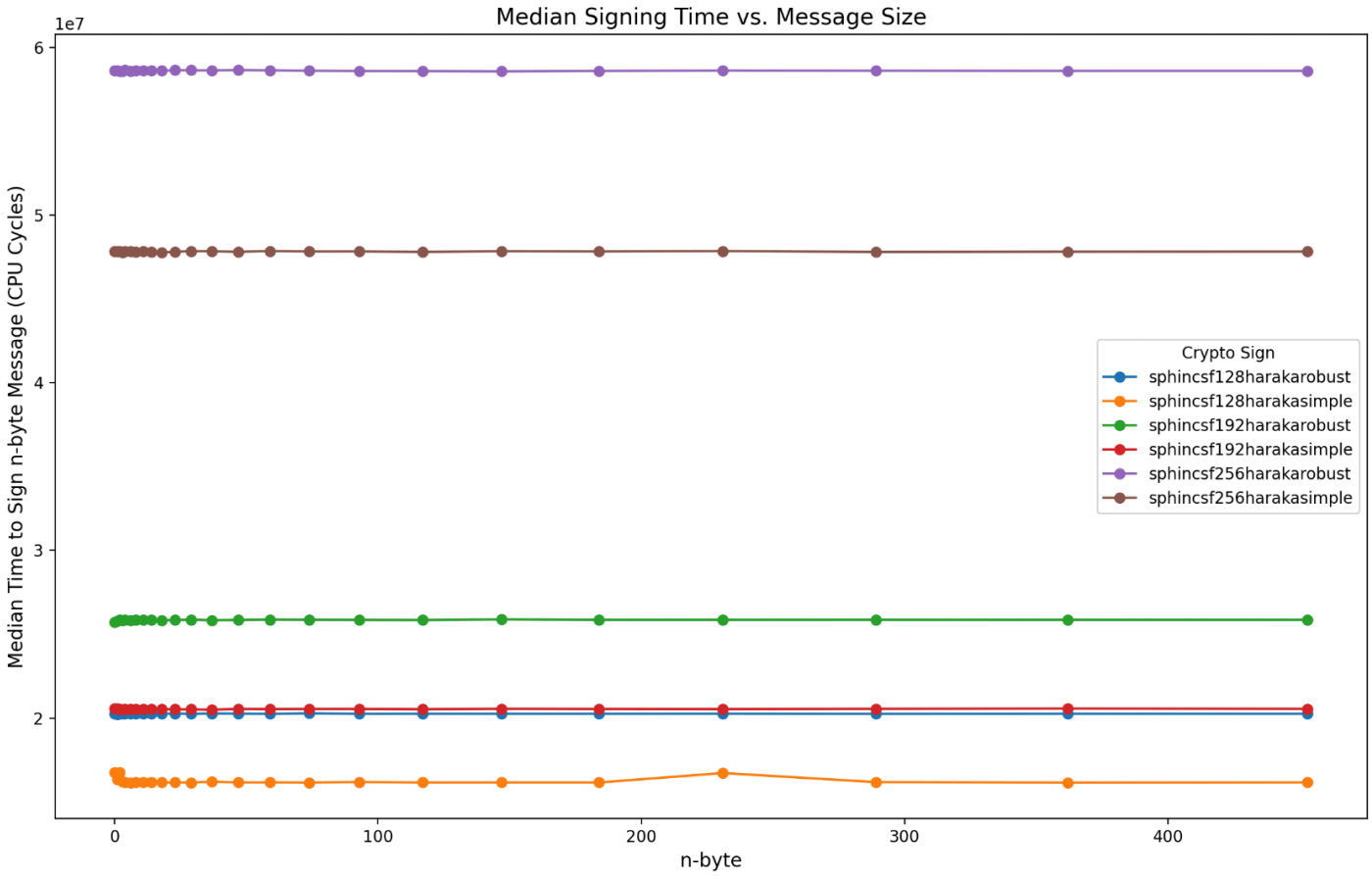
Sphincs-F (Haraka) Key Generation

Median Time (cycles) to generate a key pair: a secret key and a corresponding public key.



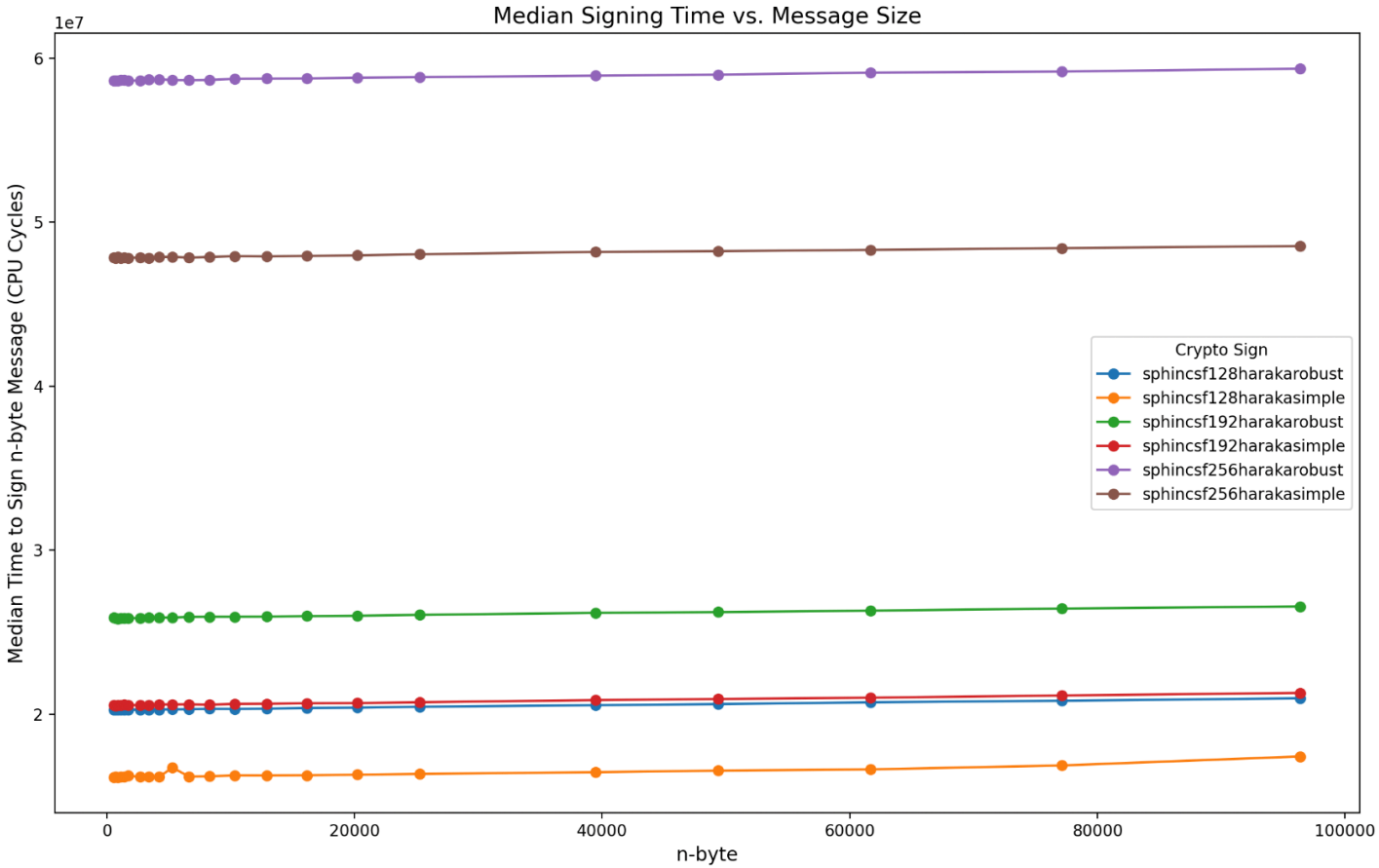
Sphincs-F (Haraka) Signing Time - 0-byte ≤ Messages ≤ 453-bytes

Time (Cycles) to sign a 0-byte ≤ message ≤ 453-bytes



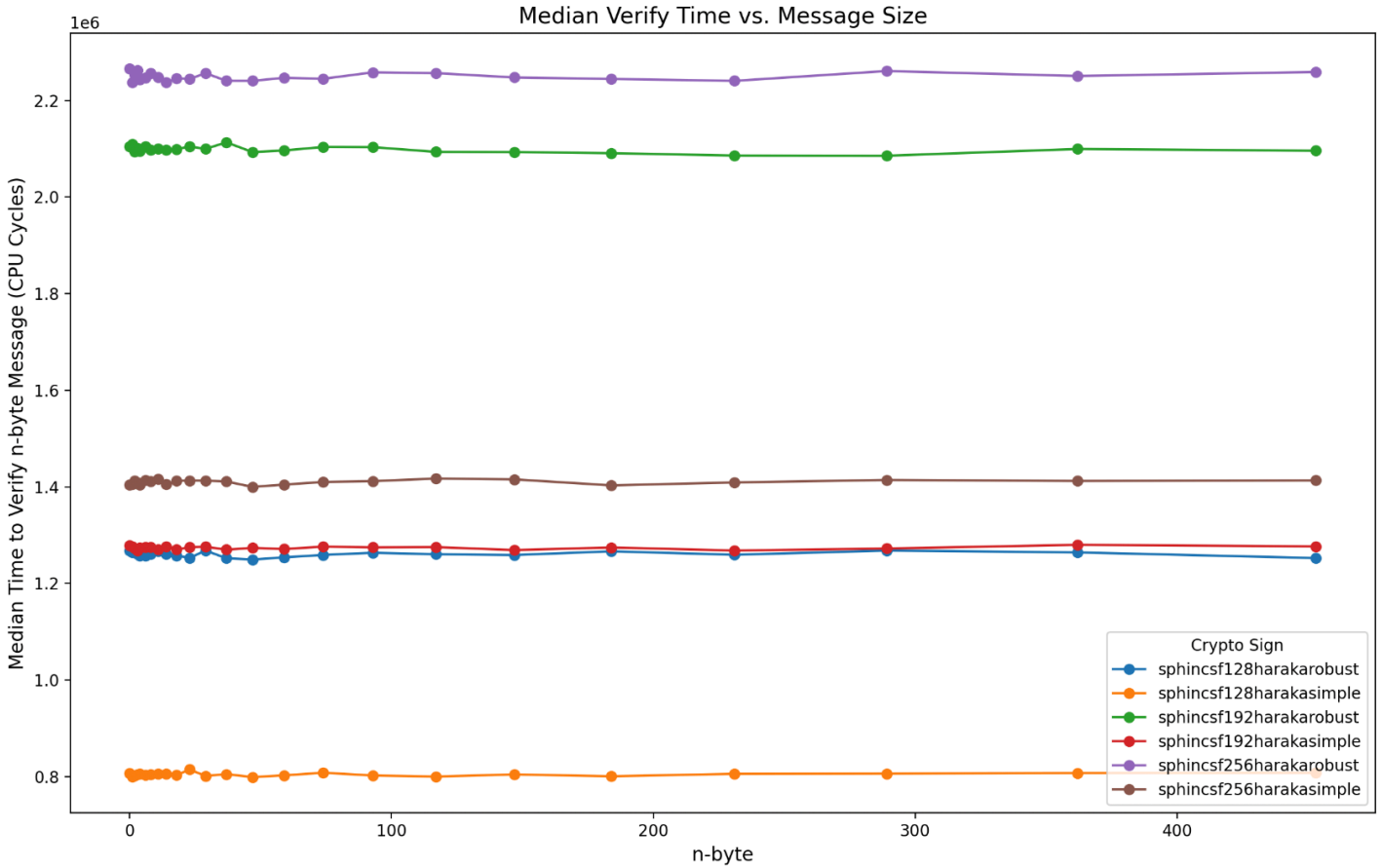
Sphincs-F (Haraka) Signing Time - 567-byte ≤ Messages ≤ 96397-byte

Time (Cycles) to sign a 567-byte ≤ message ≤ 96397-byte



Sphincs-F (Haraka) Verifying Time - 0-byte ≤ Messages ≤ 453-bytes

Time (Cycles) to open a 0-byte ≤ message ≤ 453-bytes



Sphincs-F (Haraka) Verifying Time - 567-byte ≤ Messages ≤ 96397-byte

Time (Cycles) to open a 567-byte ≤ message ≤ 96397-byte