

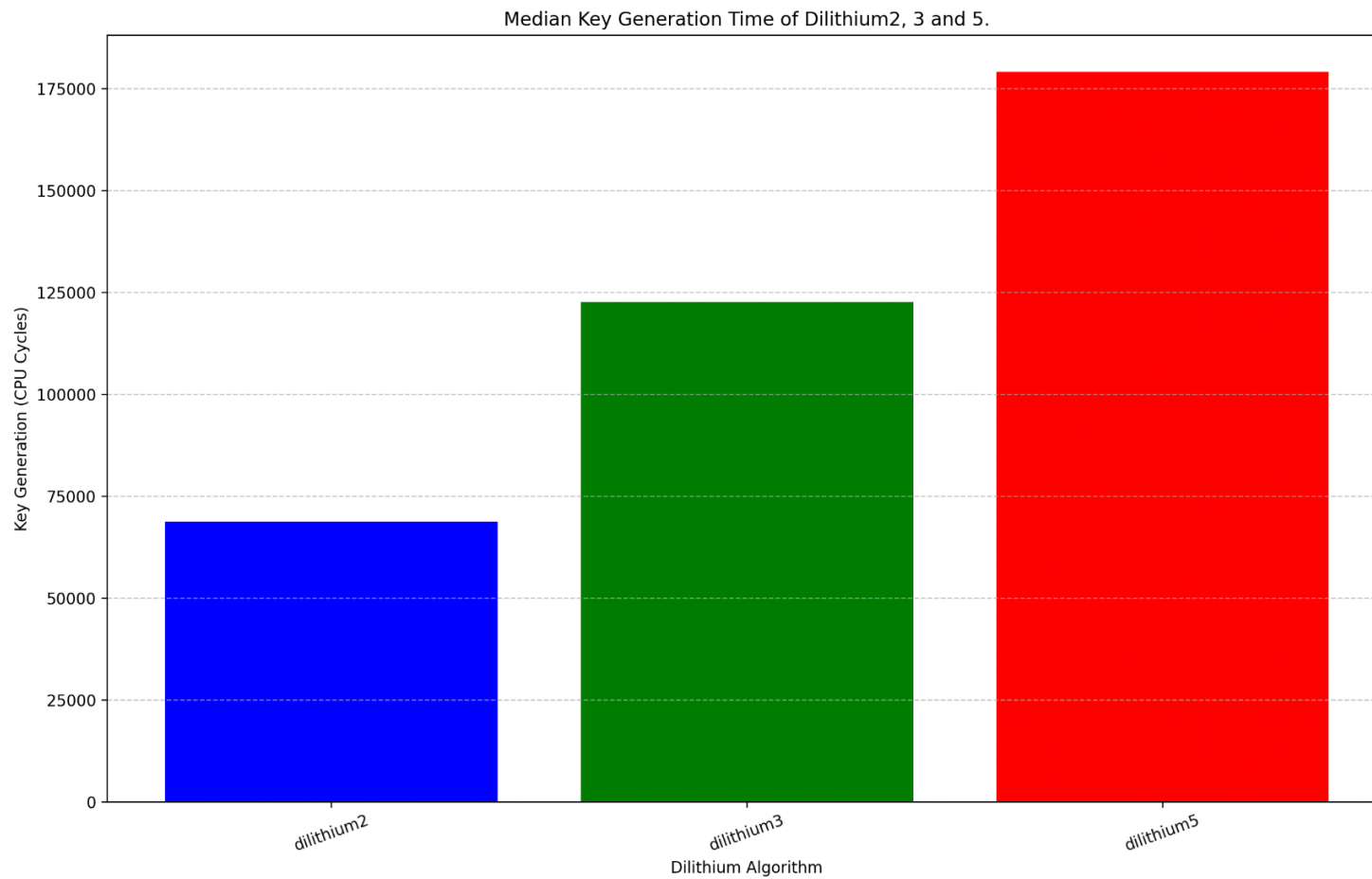
# Digital Signature Post-Quantum Algorithms Performance

<b>Dilithium</b> .....	<b>2</b>
Dilithium Key Generation.....	2
Dilithium Signing Time - 0-byte $\leq$ Messages $\leq$ 453-bytes.....	3
Dilithium Signing Time - 567-byte $\leq$ Messages $\leq$ 96397-byte.....	4
Dilithium Verifying Time - 0-byte $\leq$ Messages $\leq$ 453-bytes.....	5
Dilithium Verifying Time - 567-byte $\leq$ Messages $\leq$ 96397-byte.....	6
<b>Falcon (Tree/Dyn)</b> .....	<b>7</b>
Falcon Key Generation.....	7
Falcon Signing Time - 0-byte $\leq$ Messages $\leq$ 453-bytes.....	8
Falcon Signing Time - 567-byte $\leq$ Messages $\leq$ 96397-byte.....	9
Falcon Verifying Time - 0-byte $\leq$ Messages $\leq$ 453-bytes.....	10
Falcon Verifying Time - 567-byte $\leq$ Messages $\leq$ 96397-byte.....	11
<b>Sphincs-F (Shake256)</b> .....	<b>12</b>
Sphincs-F (Shake256) Key Generation.....	12
Sphincs-F (Shake256) Signing Time - 0-byte $\leq$ Messages $\leq$ 453-bytes.....	13
Sphincs-F (Shake256) Signing Time - 567-byte $\leq$ Messages $\leq$ 96397-byte.....	14
Sphincs-F (Shake256) Verifying Time - 0-byte $\leq$ Messages $\leq$ 453-bytes.....	15
Sphincs-F (Shake256) Verifying Time - 567-byte $\leq$ Messages $\leq$ 96397-byte.....	16
<b>Sphincs-F (Haraka)</b> .....	<b>17</b>
Sphincs-F (Haraka) Key Generation.....	17
Sphincs-F (Haraka) Signing Time - 0-byte $\leq$ Messages $\leq$ 453-bytes.....	18
Sphincs-F (Haraka) Signing Time - 567-byte $\leq$ Messages $\leq$ 96397-byte.....	19
Sphincs-F (Haraka) Verifying Time - 0-byte $\leq$ Messages $\leq$ 453-bytes.....	20
Sphincs-F (Haraka) Verifying Time - 567-byte $\leq$ Messages $\leq$ 96397-byte.....	21

# Dilithium

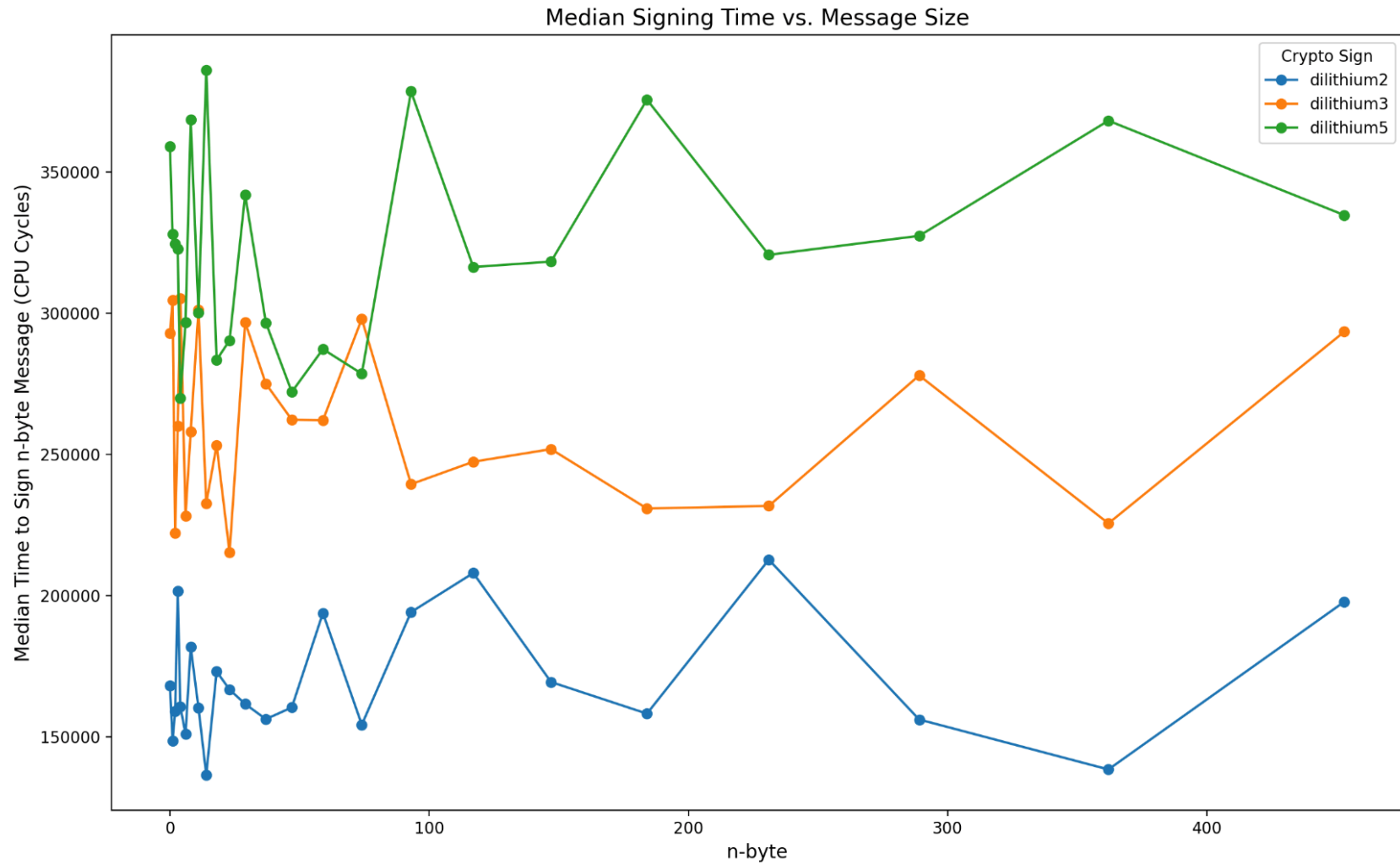
## Dilithium Key Generation

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



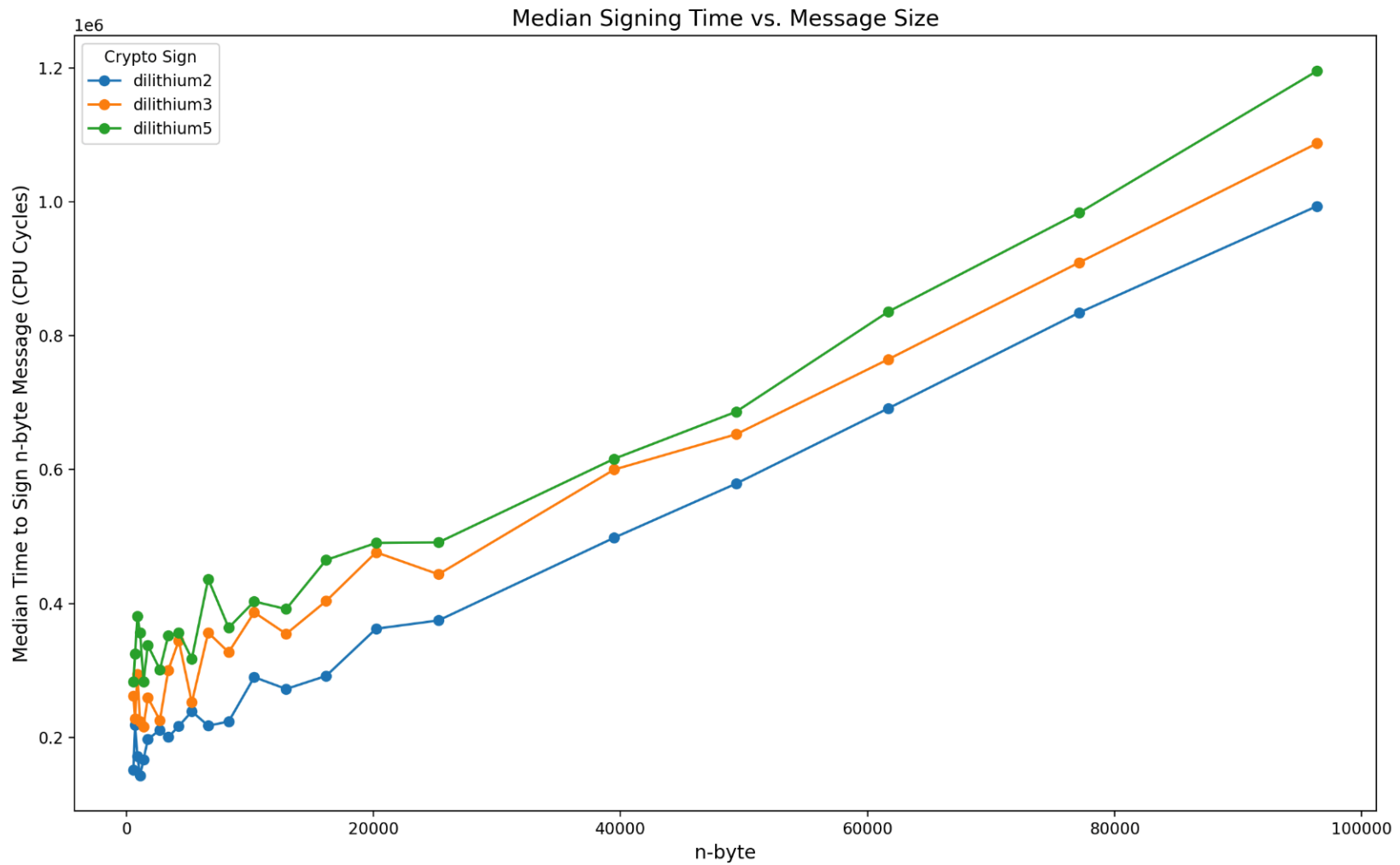
## Dilithium Signing Time - 0-byte $\leq$ Messages $\leq$ 453-bytes

Time (Cycles) to sign a 0-byte  $\leq$  message  $\leq$  453-bytes



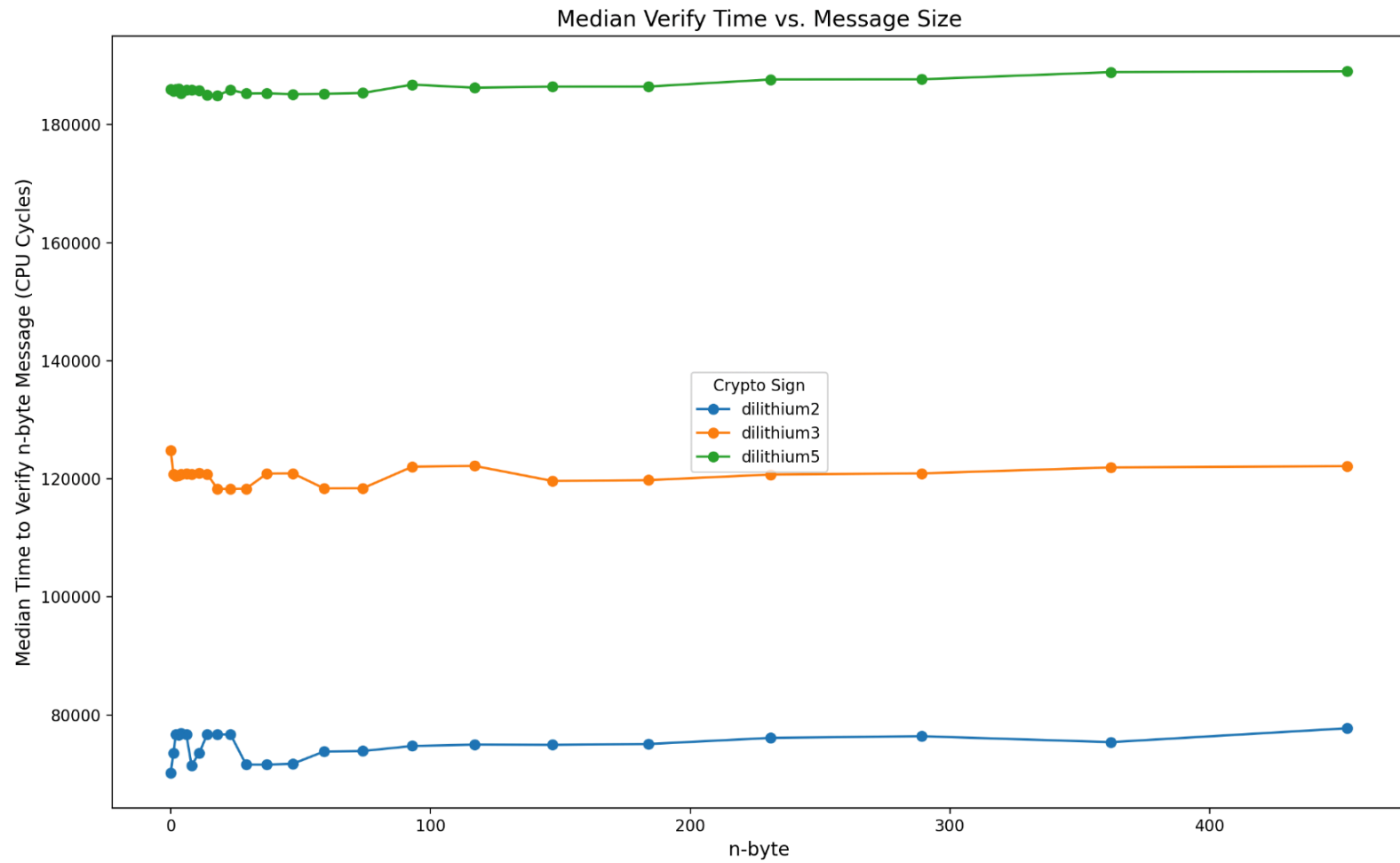
## Dilithium Signing Time - 567-byte $\leq$ Messages $\leq$ 96397-byte

Time (Cycles) to sign a 567-byte  $\leq$  message  $\leq$  96397-byte



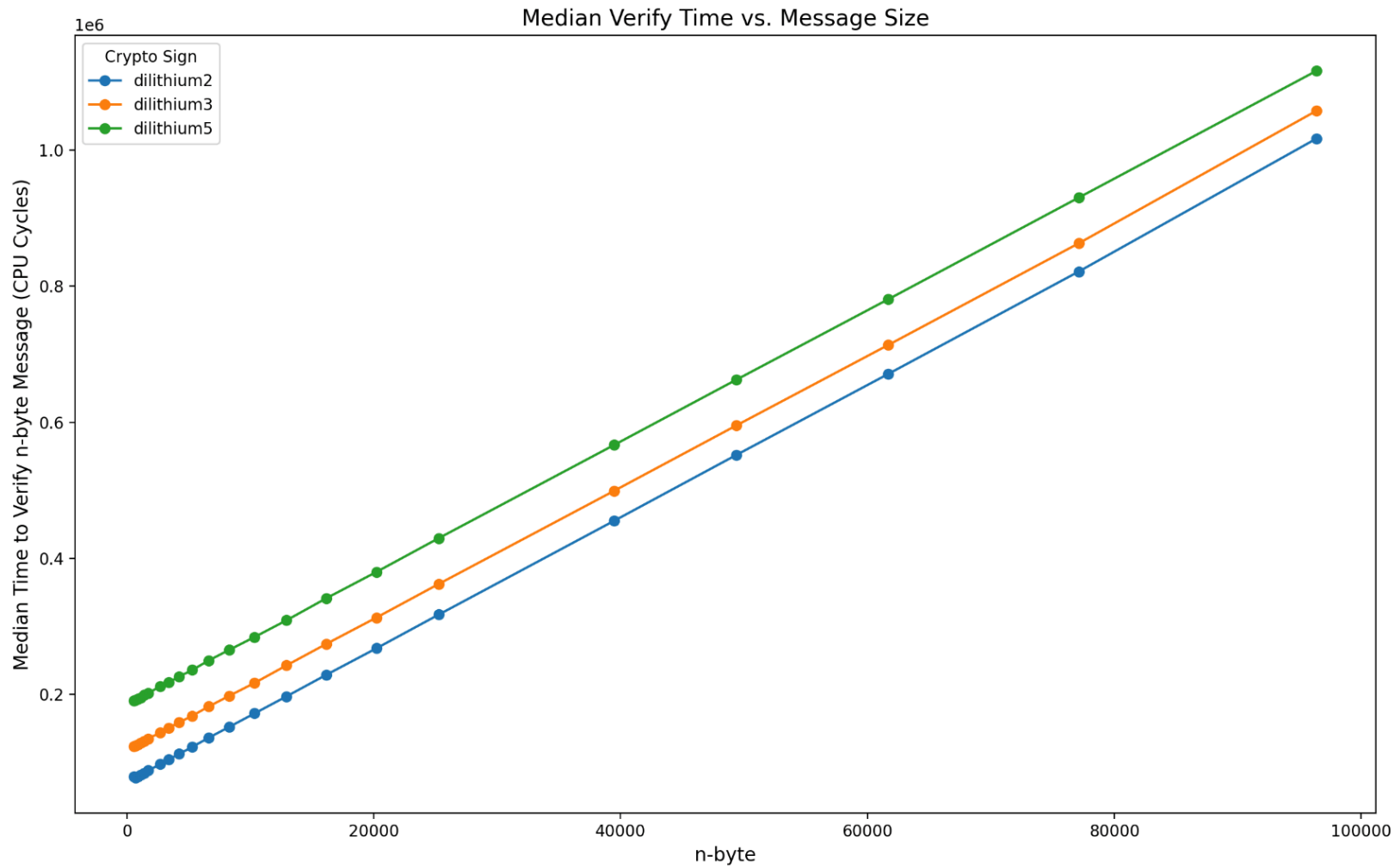
## Dilithium Verifying Time - 0-byte $\leq$ Messages $\leq$ 453-bytes

Time (Cycles) to open a 0-byte  $\leq$  message  $\leq$  453-bytes



## Dilithium Verifying Time - 567-byte $\leq$ Messages $\leq$ 96397-byte

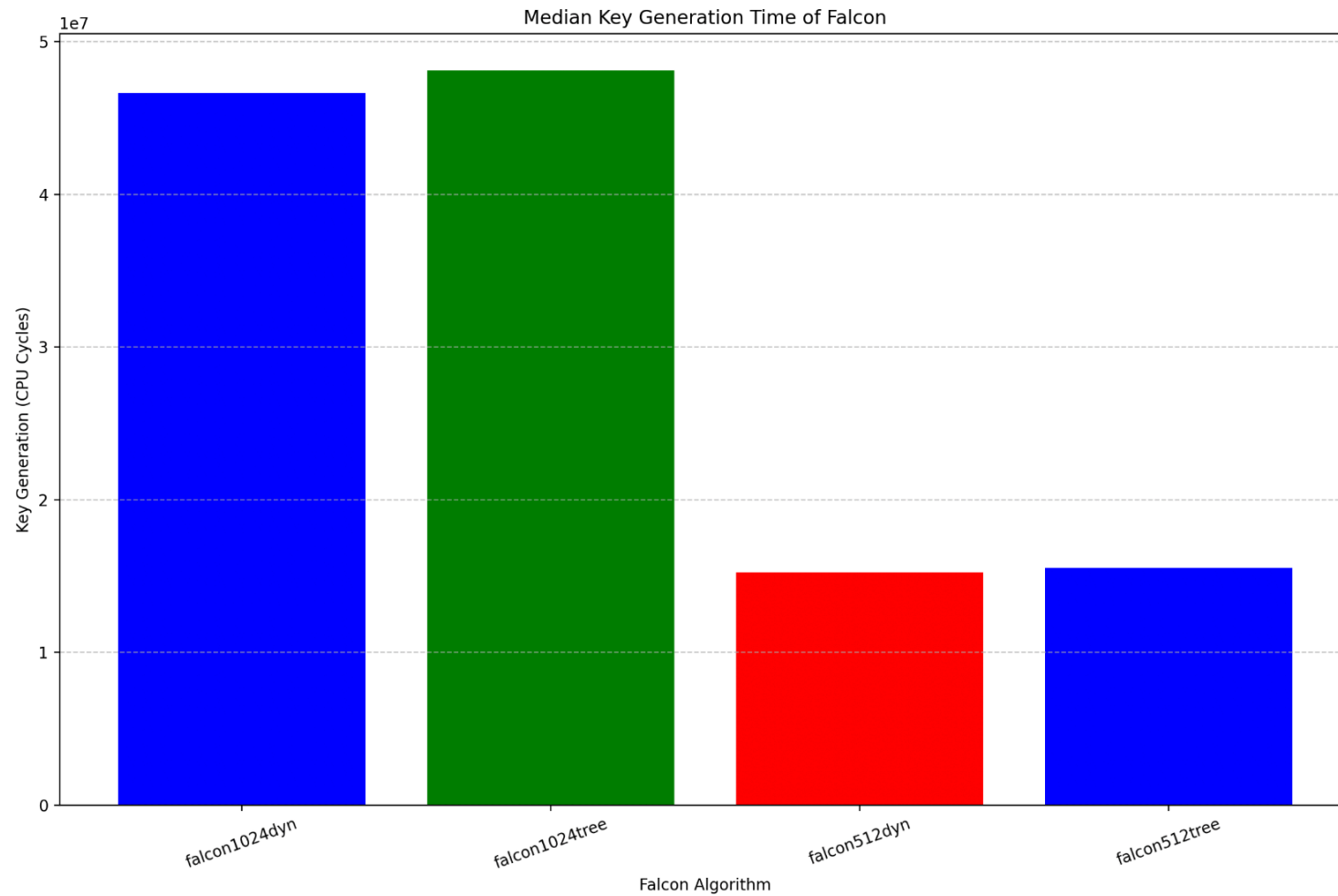
Time (Cycles) to open a 567-byte  $\leq$  message  $\leq$  96397-byte



# Falcon (Tree/Dyn)

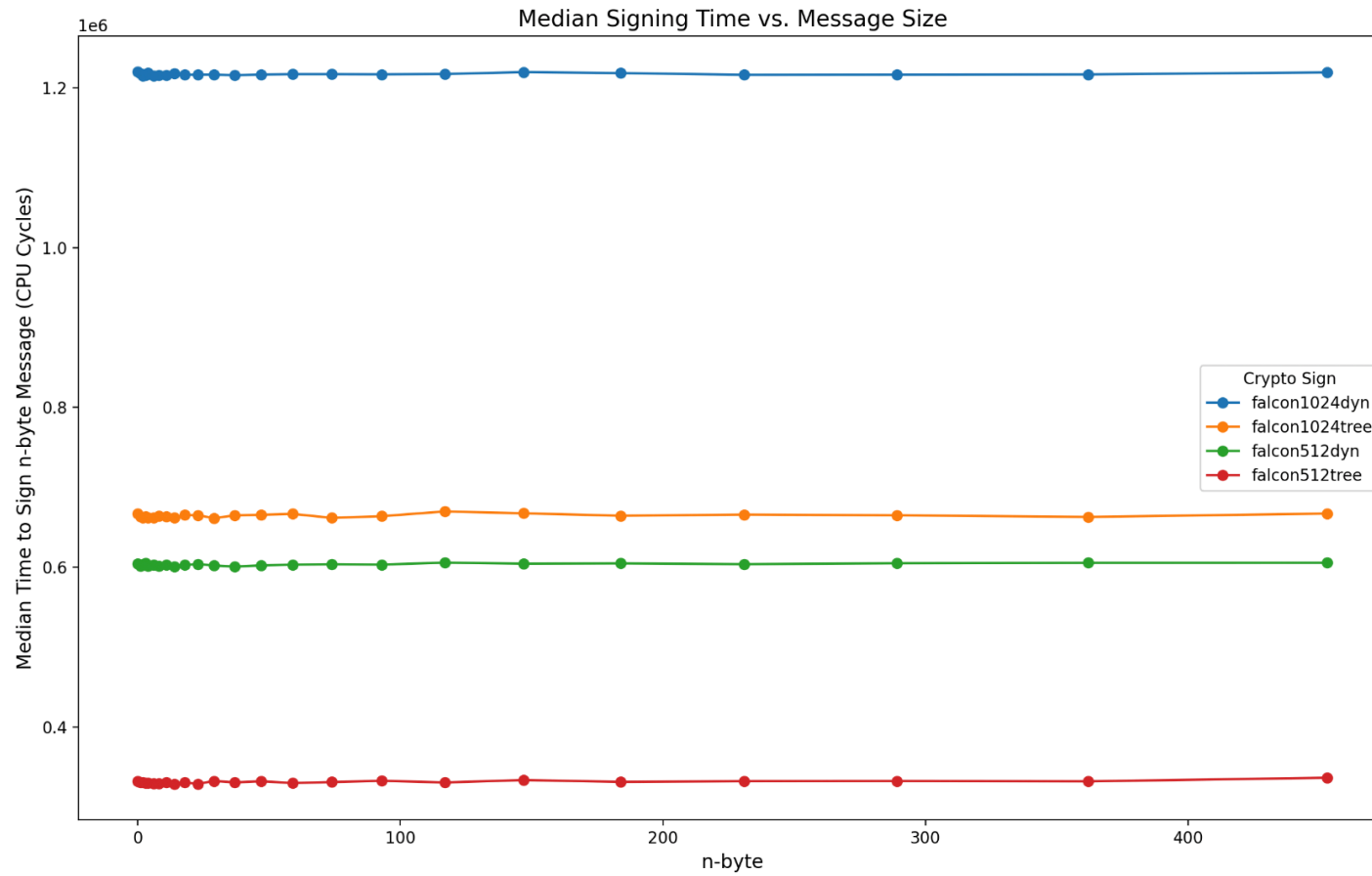
## Falcon Key Generation

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



## Falcon Signing Time - 0-byte $\leq$ Messages $\leq$ 453-bytes

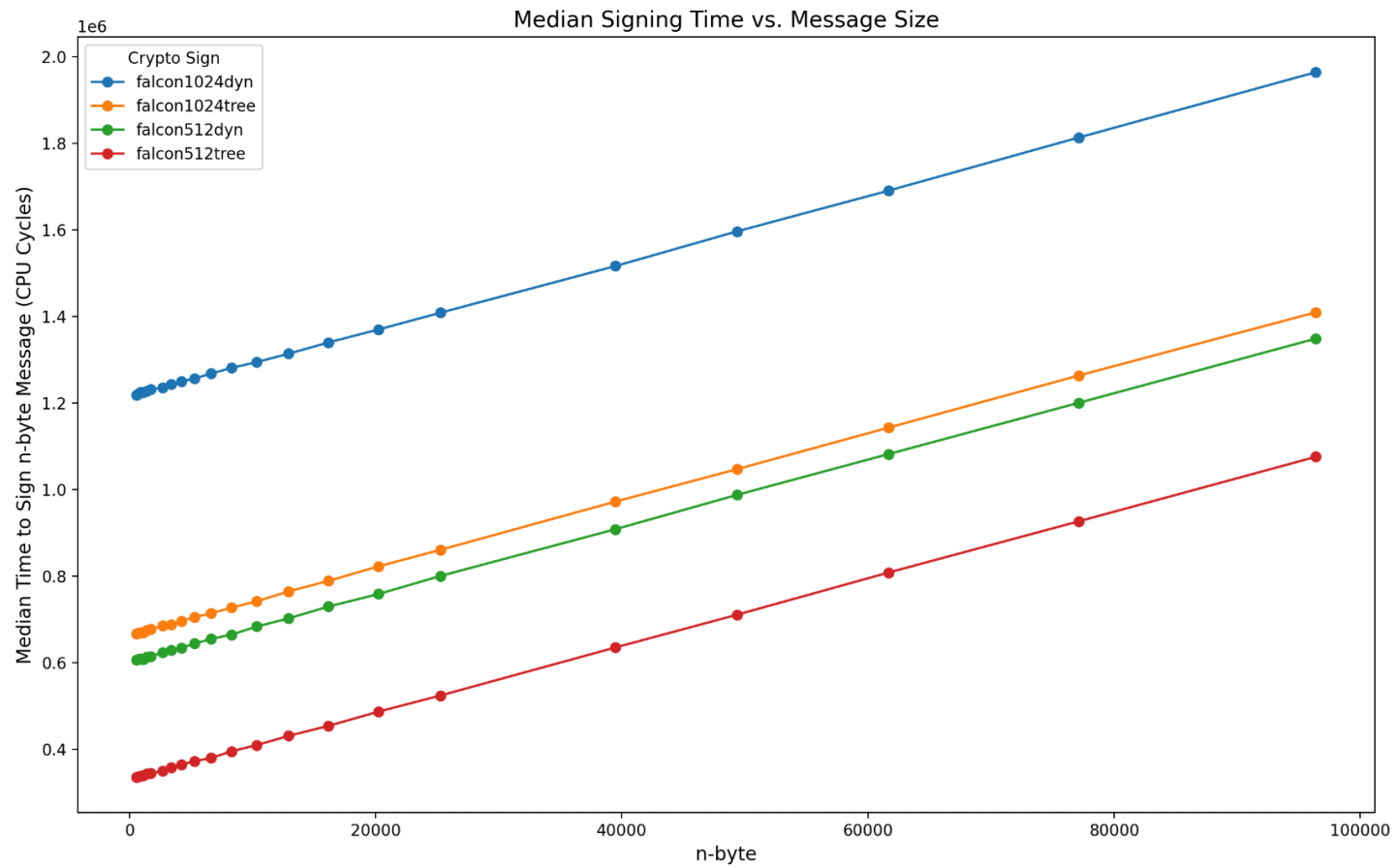
Time (Cycles) to sign a 0-byte  $\leq$  message  $\leq$  453-bytes





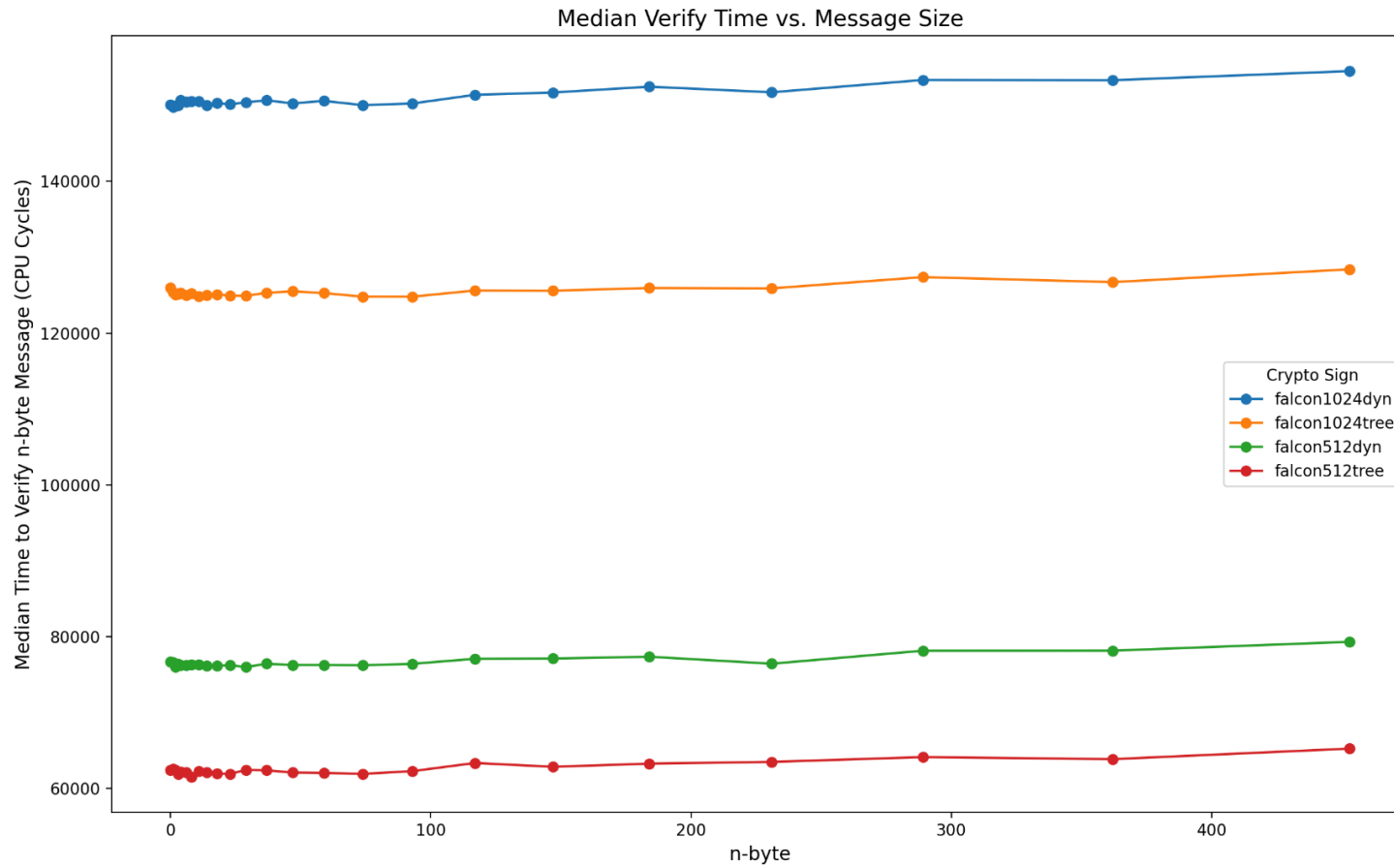
## Falcon Signing Time - 567-byte $\leq$ Messages $\leq$ 96397-byte

Time (Cycles) to sign a 567-byte  $\leq$  message  $\leq$  96397-byte



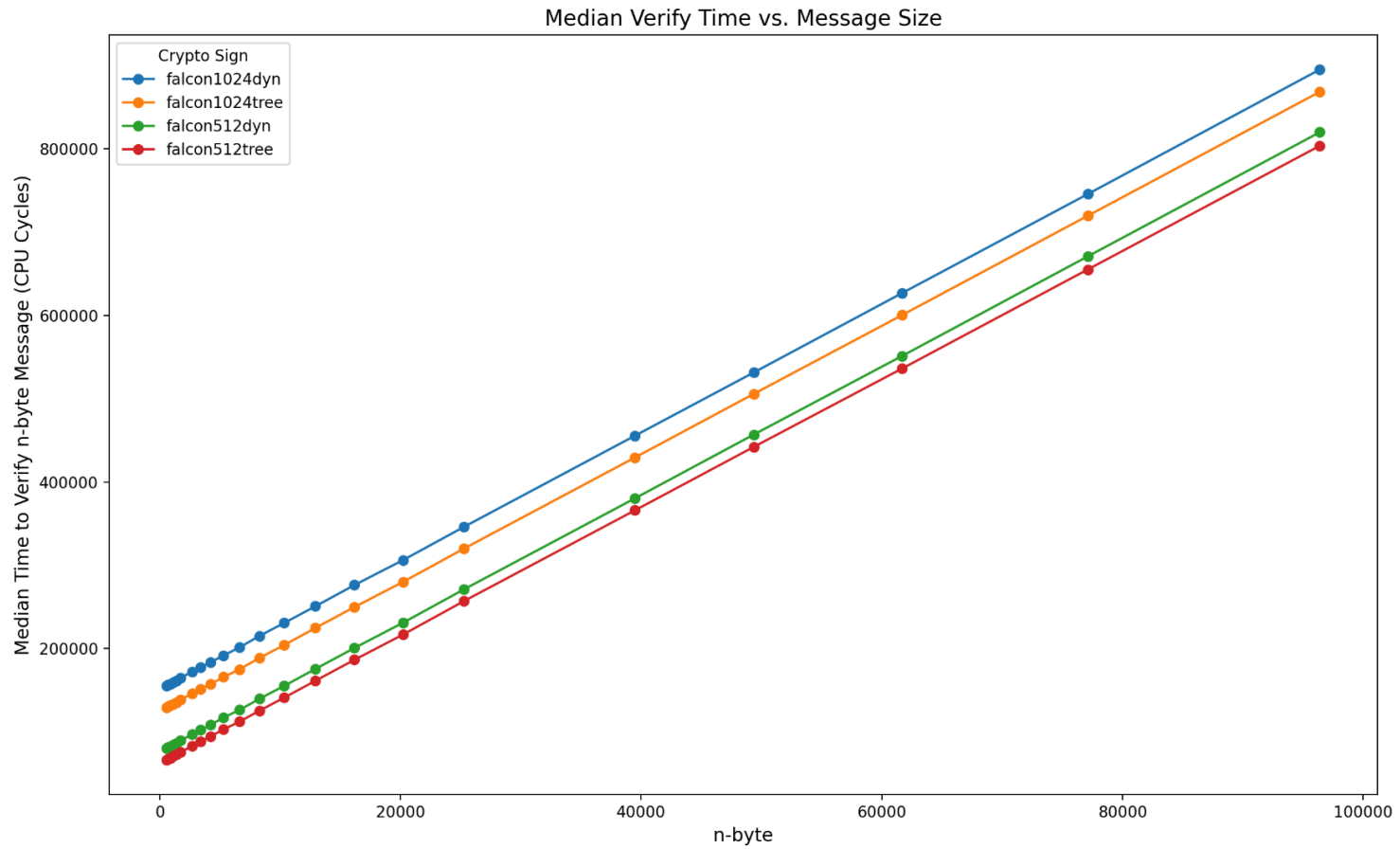
## Falcon Verifying Time - 0-byte $\leq$ Messages $\leq$ 453-bytes

Time (Cycles) to open a 0-byte  $\leq$  message  $\leq$  453-bytes



## Falcon Verifying Time - 567-byte $\leq$ Messages $\leq$ 96397-byte

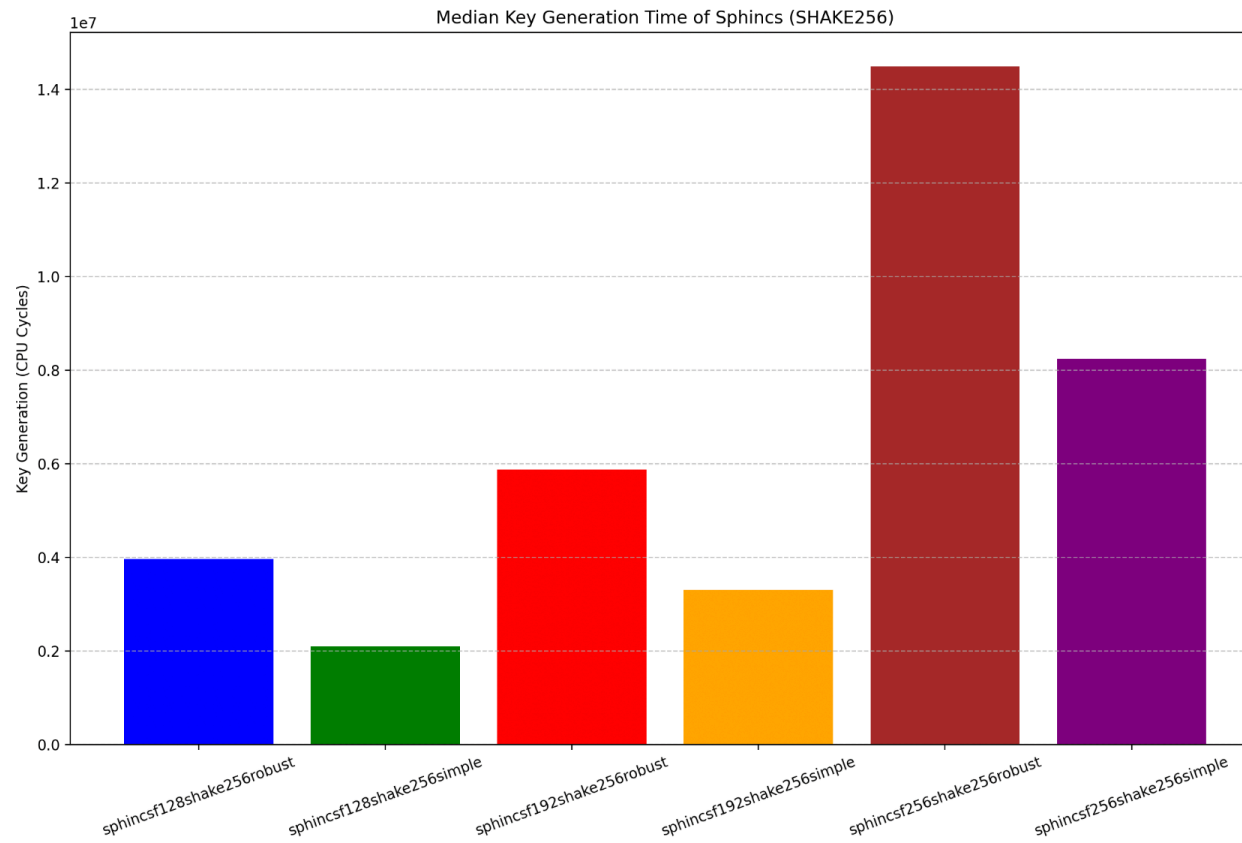
Time (Cycles) to open a 567-byte  $\leq$  message  $\leq$  96397-byte



# Sphincs-F (Shake256)

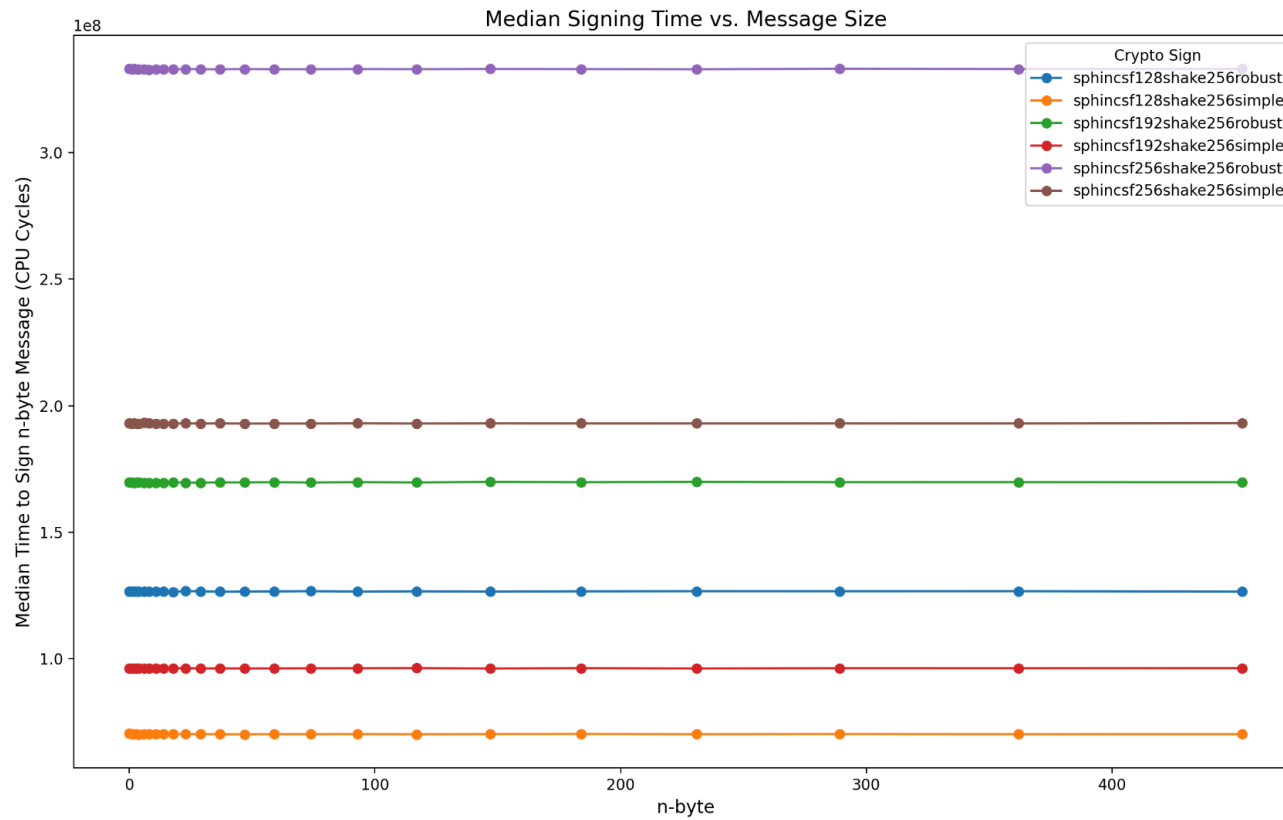
## Sphincs-F (Shake256) Key Generation

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



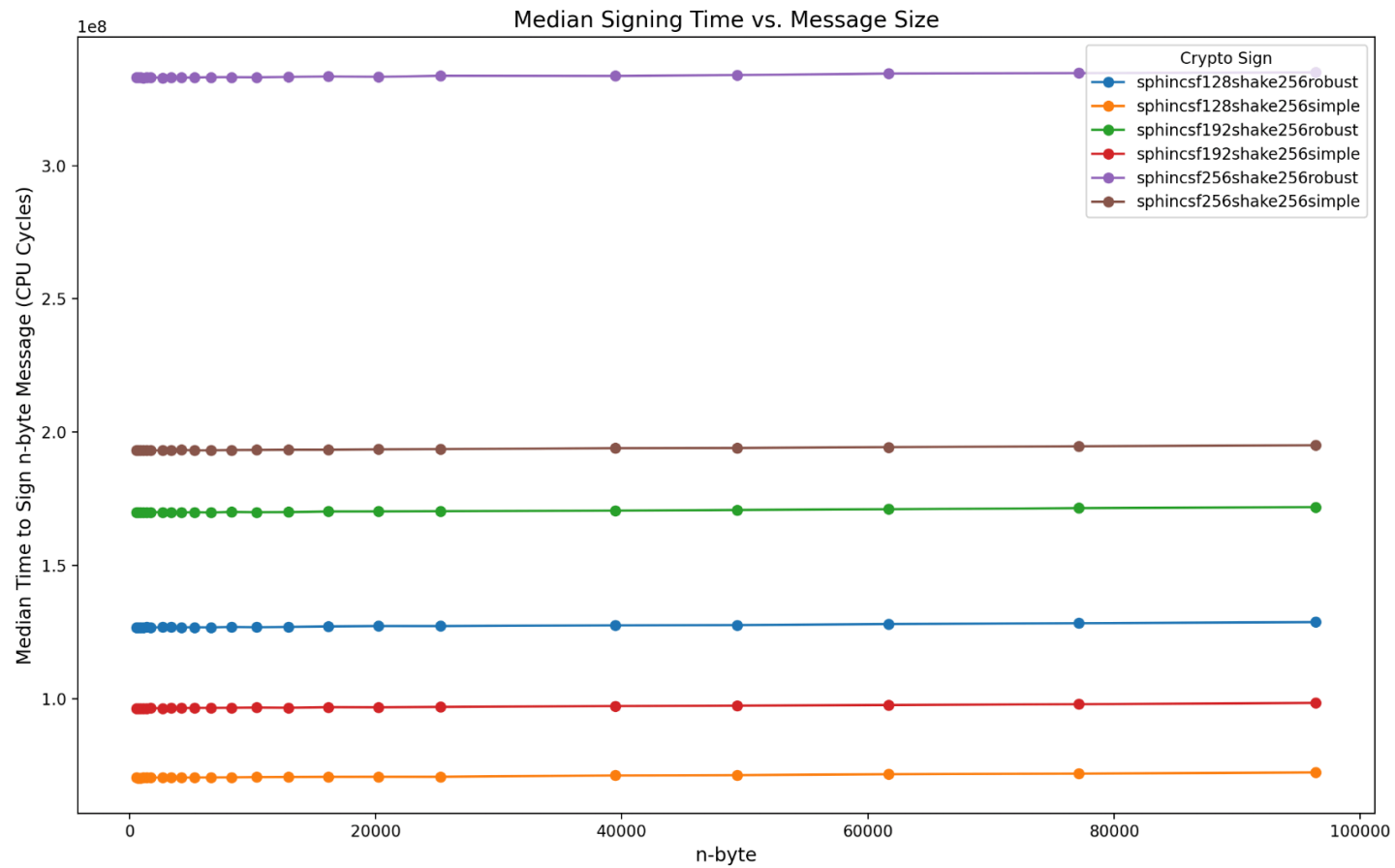
## Sphincs-F (Shake256) Signing Time - 0-byte $\leq$ Messages $\leq$ 453-bytes

Time (Cycles) to sign a 0-byte  $\leq$  message  $\leq$  453-bytes



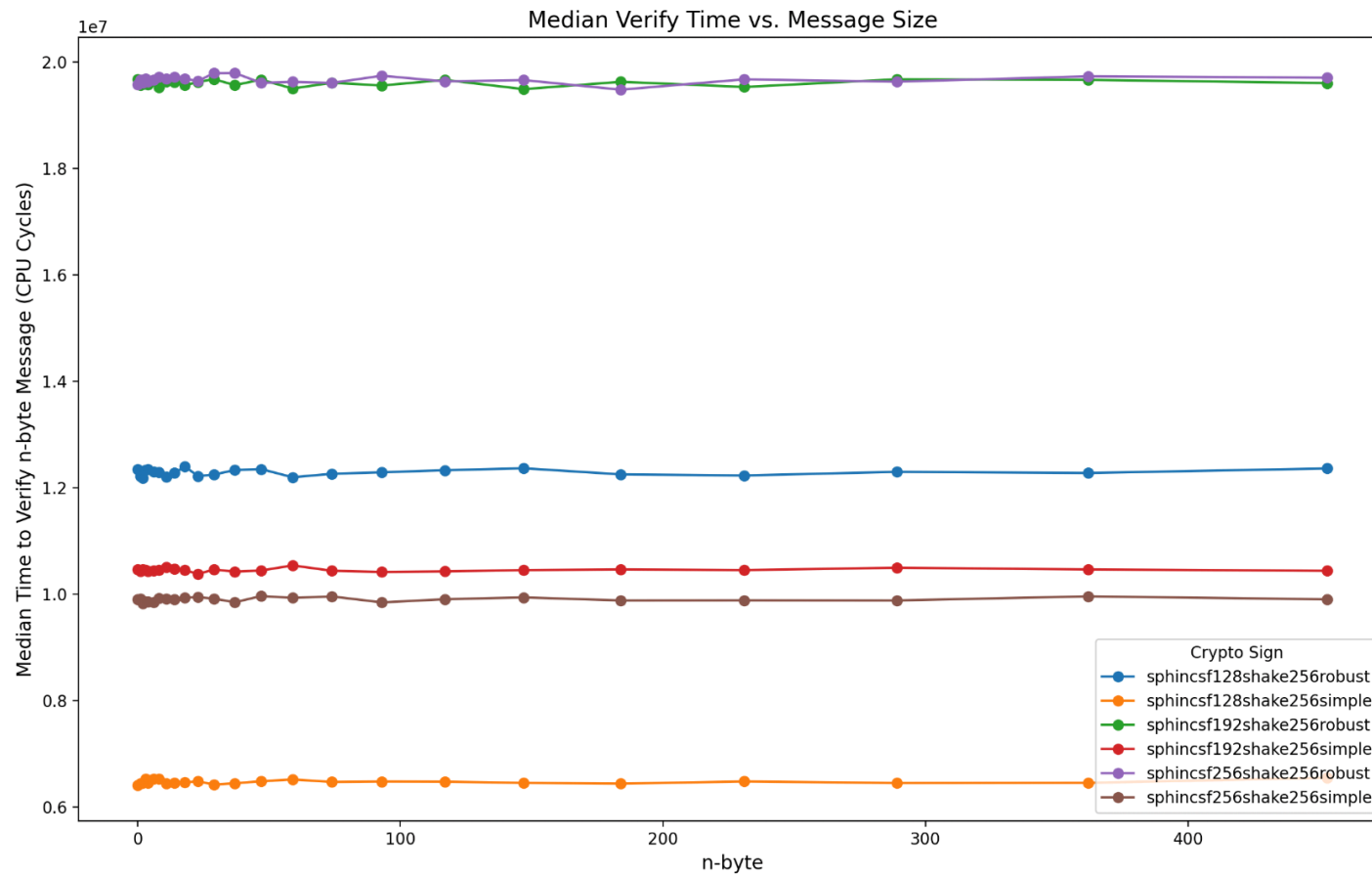
## Sphincs-F (Shake256) Signing Time - 567-byte ≤ Messages ≤ 96397-byte

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



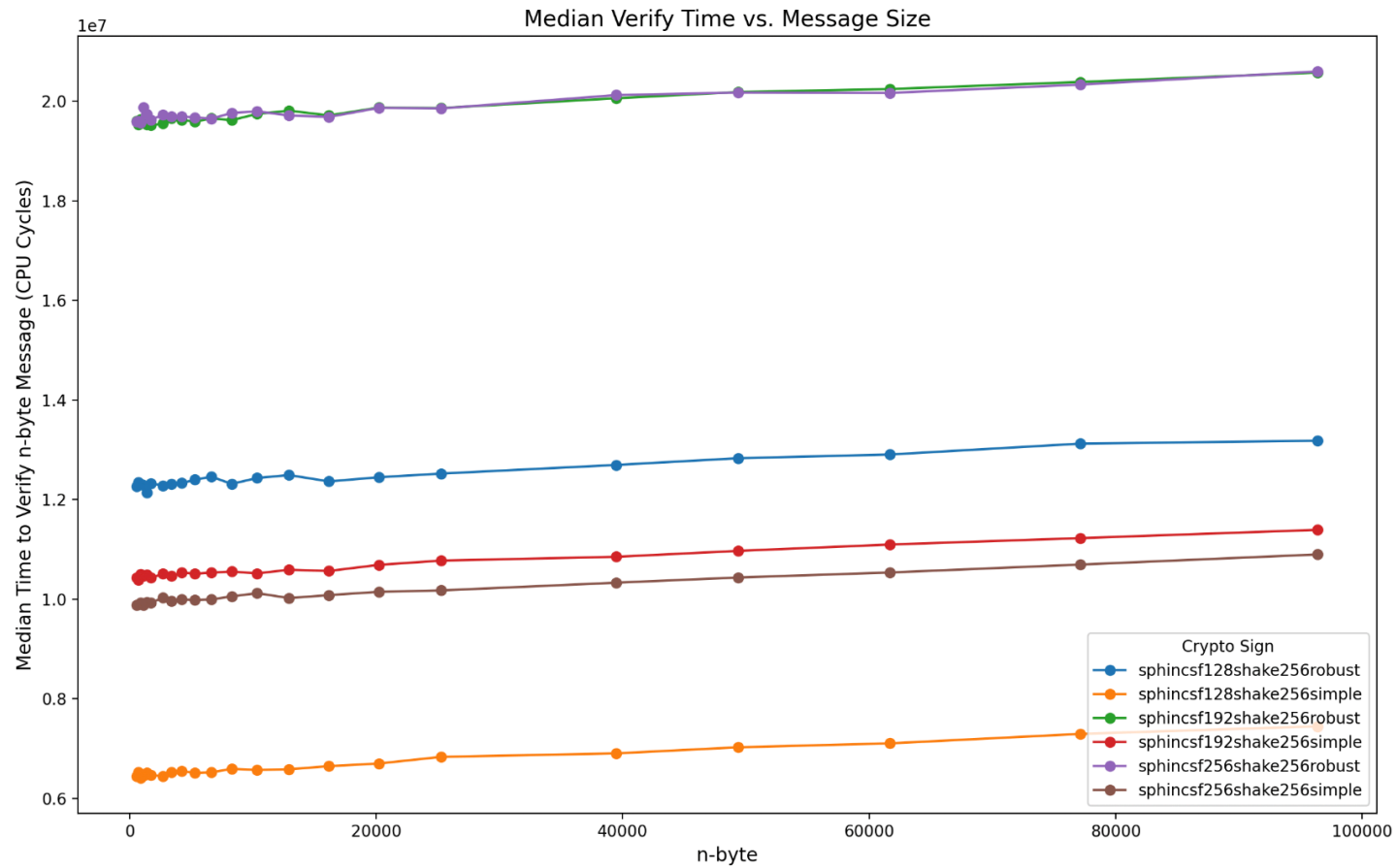
## Sphincs-F (Shake256) Verifying Time - 0-byte $\leq$ Messages $\leq$ 453-bytes

Time (Cycles) to open a 0-byte  $\leq$  message  $\leq$  453-bytes



## Sphincs-F (Shake256) Verifying Time - 567-byte $\leq$ Messages $\leq$ 96397-byte

Time (Cycles) to open a 567-byte  $\leq$  message  $\leq$  96397-byte

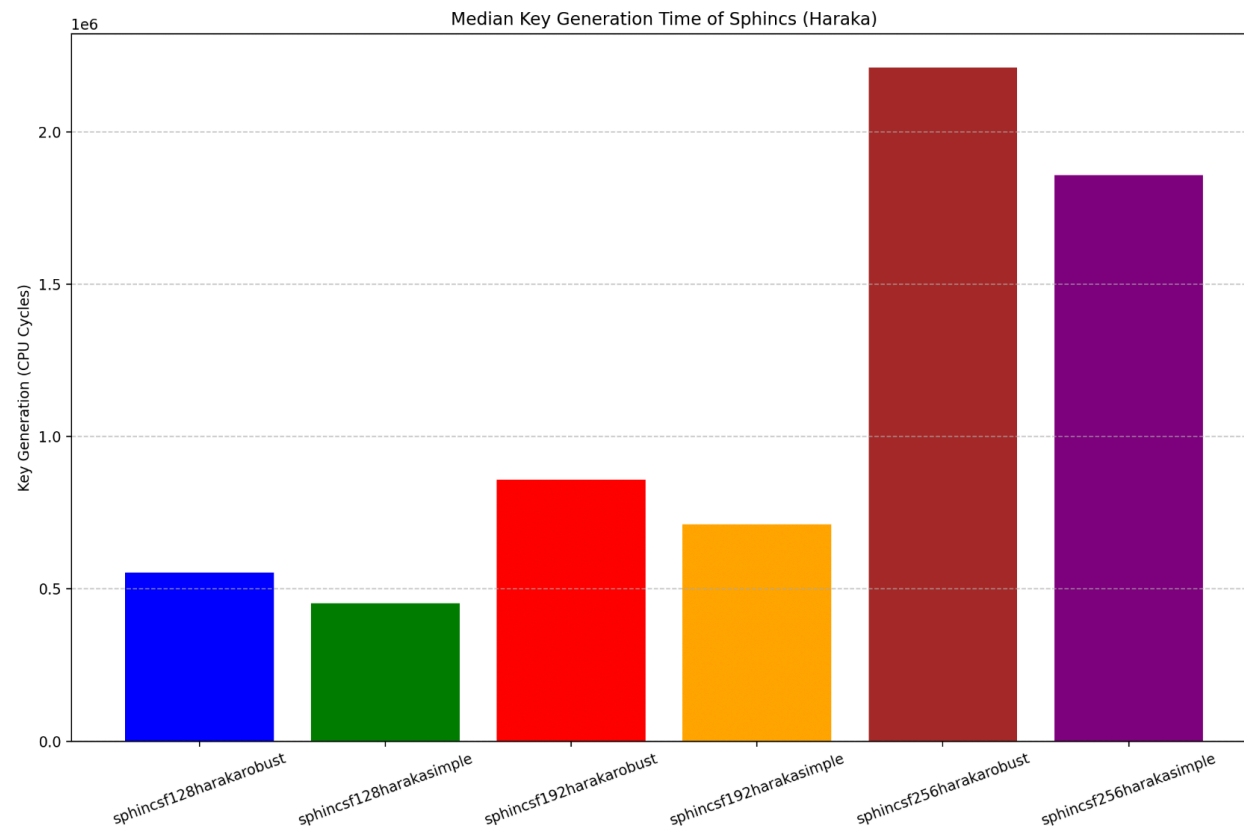




# Sphincs-F (Haraka)

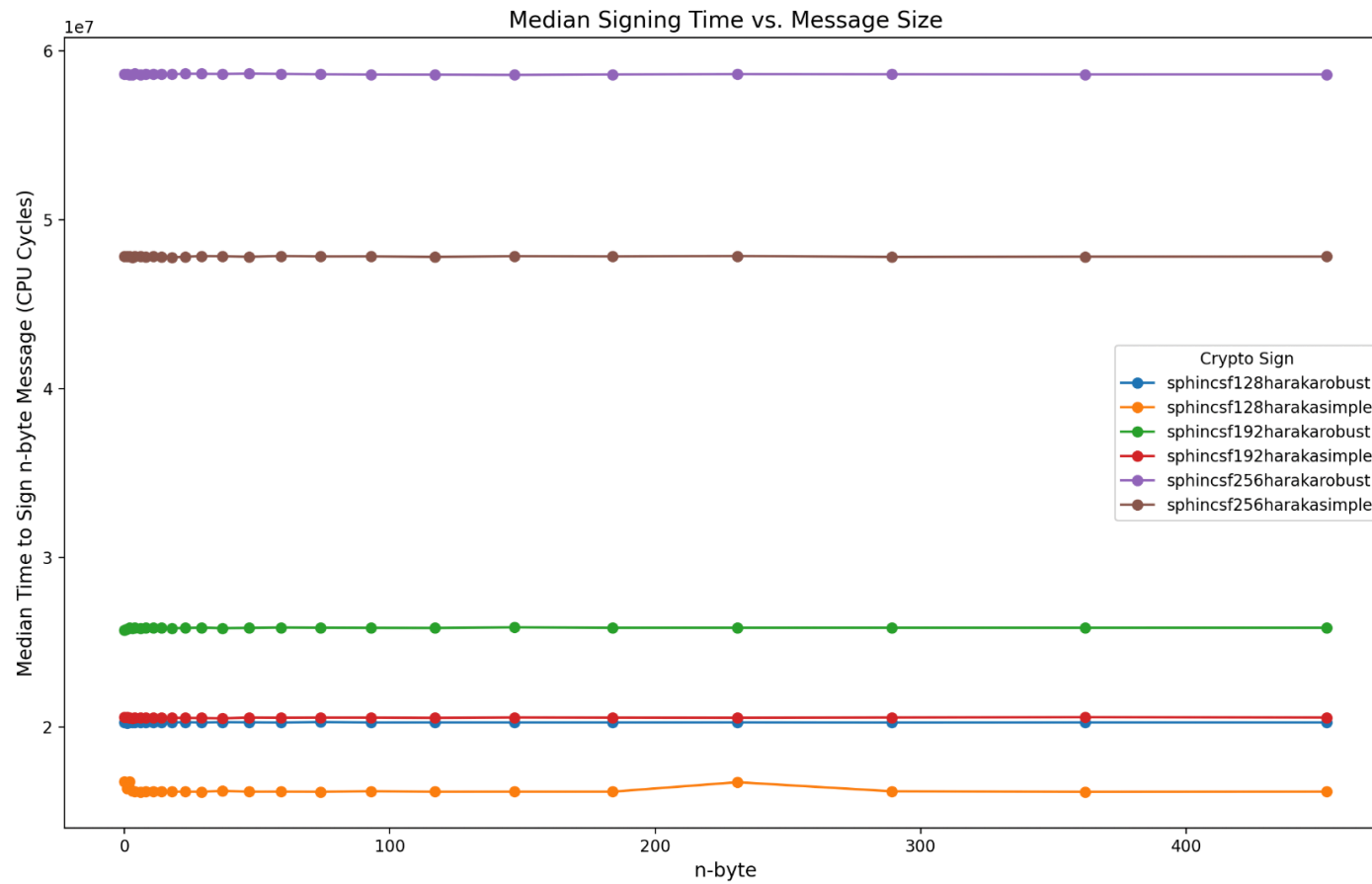
## Sphincs-F (Haraka) Key Generation

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



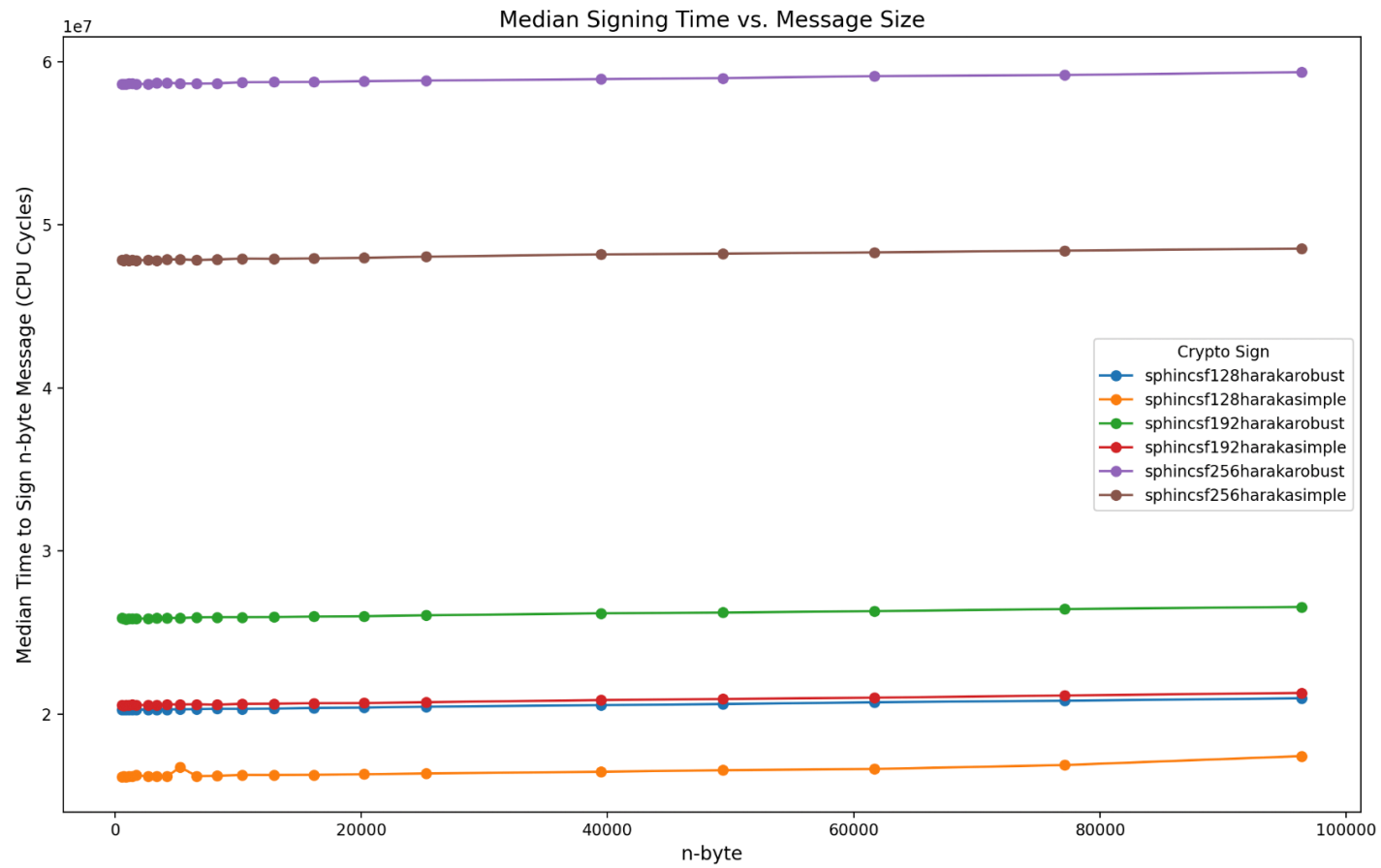
## Sphincs-F (Haraka) Signing Time - 0-byte $\leq$ Messages $\leq$ 453-bytes

Time (Cycles) to sign a 0-byte  $\leq$  message  $\leq$  453-bytes



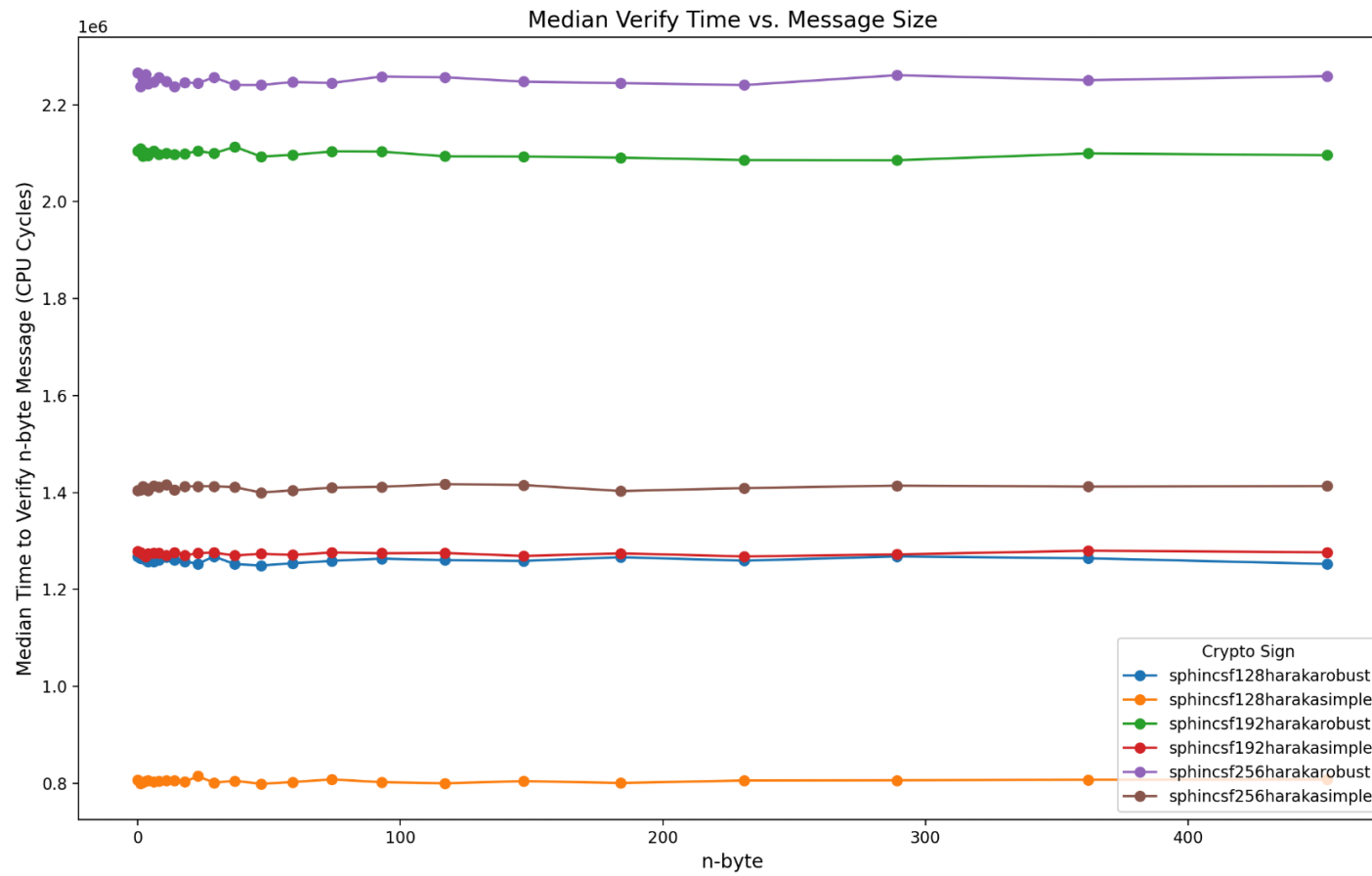
## Sphincs-F (Haraka) Signing Time - 567-byte $\leq$ Messages $\leq$ 96397-byte

Time (Cycles) to sign a 567-byte  $\leq$  message  $\leq$  96397-byte



## Sphincs-F (Haraka) Verifying Time - 0-byte $\leq$ Messages $\leq$ 453-bytes

Time (Cycles) to open a 0-byte  $\leq$  message  $\leq$  453-bytes



## Sphincs-F (Haraka) Verifying Time - 567-byte $\leq$ Messages $\leq$ 96397-byte

Time (Cycles) to open a 567-byte  $\leq$  message  $\leq$  96397-byte

