Some SUPERCOP results

Overview

Will show signature graphs and KEM graphs covering AIMer, HAETAE, MQ-Sign, NCC-Sign, NTRU+, SMAUG-T, and selected baselines for comparison.

Overview

Will show signature graphs and KEM graphs covering AIMer, HAETAE, MQ-Sign, NCC-Sign, NTRU+, SMAUG-T, and selected baselines for comparison. Some warnings:

- Graphs are for Intel Haswell (2013) and AMD Zen 3 (2020). Other CPUs can have different performance.

Overview

Will show signature graphs and KEM graphs covering AIMer, HAETAE, MQ-Sign, NCC-Sign, NTRU+, SMAUG-T, and selected baselines for comparison. Some warnings:

- Graphs are for Intel Haswell (2013) and AMD Zen 3 (2020). Other CPUs can have different performance.
- Timings in these graphs are medians.

Overview

Will show signature graphs and KEM graphs covering AIMer, HAETAE, MQ-Sign, NCC-Sign, NTRU+, SMAUG-T, and selected baselines for comparison. Some warnings:

- Graphs are for Intel Haswell (2013) and AMD Zen 3 (2020). Other CPUs can have different performance.
- Timings in these graphs are medians.
- Often the speed for future users will be better because a future implementation is faster. Compilers generally do not produce good code.

Overview

Will show signature graphs and KEM graphs covering AIMer, HAETAE, MQ-Sign, NCC-Sign, NTRU+, SMAUG-T, and selected baselines for comparison. Some warnings:

- Graphs are for Intel Haswell (2013) and AMD Zen 3 (2020). Other CPUs can have different performance.
- Timings in these graphs are medians.
- Often the speed for future users will be better because a future implementation is faster. Compilers generally do not produce good code.
- Total cost of application includes cryptographic computation + cryptographic communication + other costs. Often a faster computation isn't better for application: e.g., outweighed by communication costs.

Overview

Will show signature graphs and KEM graphs covering AIMer, HAETAE, MQ-Sign, NCC-Sign, NTRU+, SMAUG-T, and selected baselines for comparison. Some warnings:

- Graphs are for Intel Haswell (2013) and AMD Zen 3 (2020). Other CPUs can have different performance.
- Timings in these graphs are medians.
- Often the speed for future users will be better because a future implementation is faster. Compilers generally do not produce good code.
- Total cost of application includes cryptographic computation + cryptographic communication + other costs. Often a faster computation isn't better for application: e.g., outweighed by communication costs.

See `bench.cr.yp.to` for more CPUs; quartiles; updates.

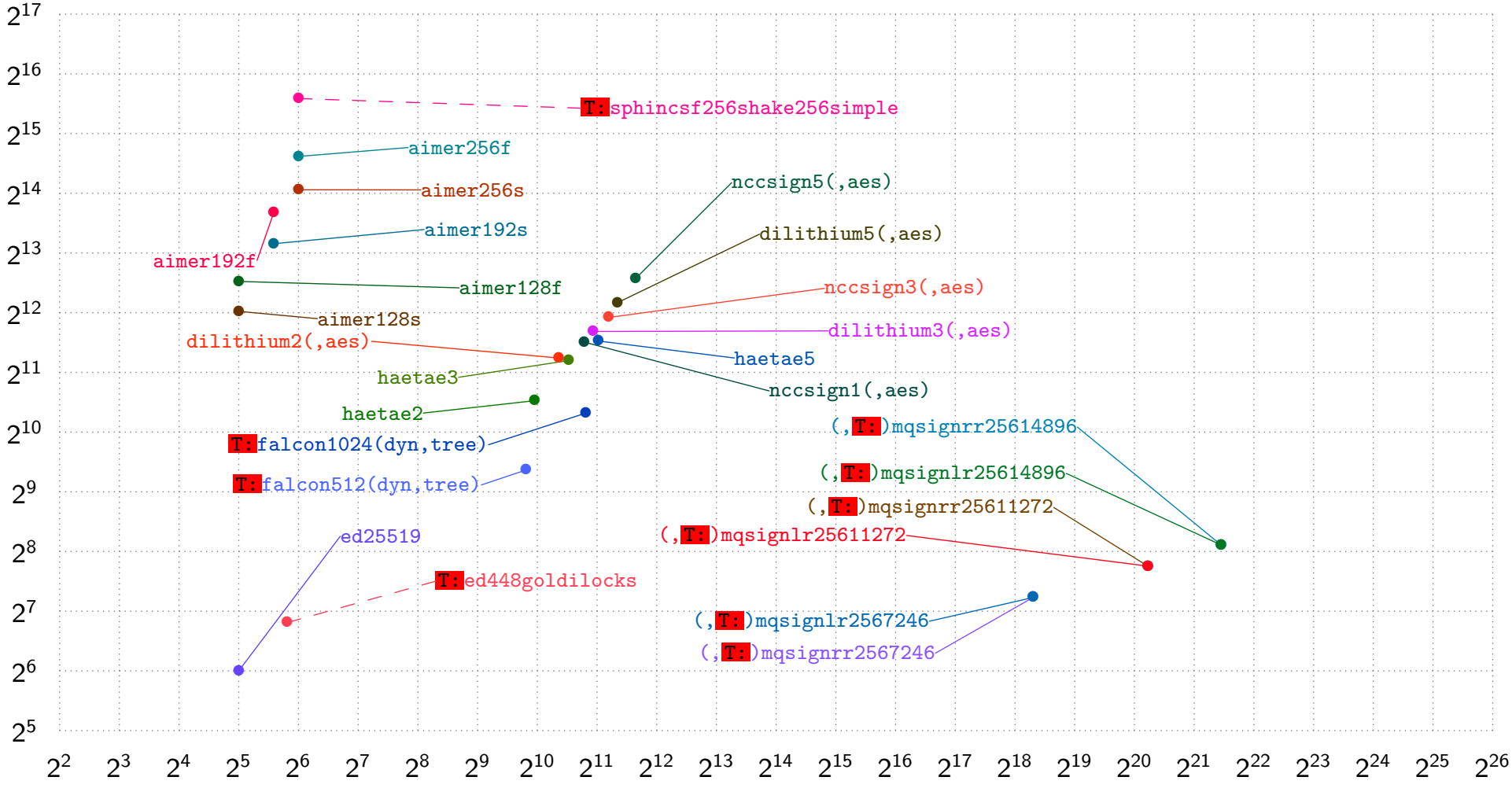
Signatures

amd64, titan0, crypto_sign, key size, signature size https://bench.cr.yp.to

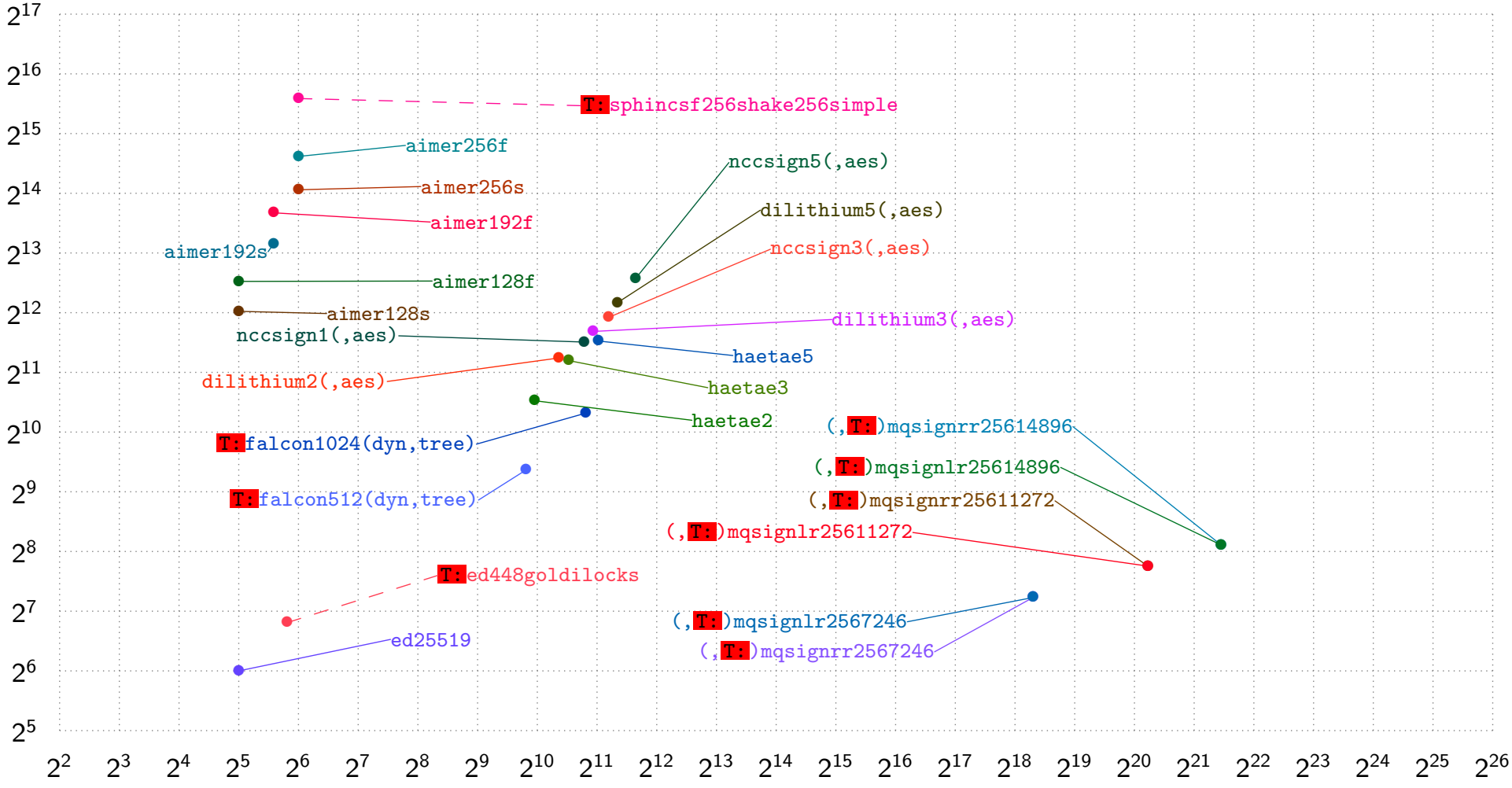
Horizontal axis: Space (bytes) for a public key (crypto_sign_PUBLICKEYBYTES). 20241021

Vertical axis: Space overhead (bytes) for signing a long message (at most crypto_sign_BYTES).

"T:" means that the SUPERCOP database does not list constant time as a goal for this implementation.



amd64, cezanne, crypto_sign, key size, signature size https://bench.cr.yp.to
Horizontal axis: Space (bytes) for a public key (crypto_sign_PUBLICKEYBYTES). 20241021
Vertical axis: Space overhead (bytes) for signing a long message (at most crypto_sign_BYTES).
"T:" means that the SUPERCOP database does not list constant time as a goal for this implementation.

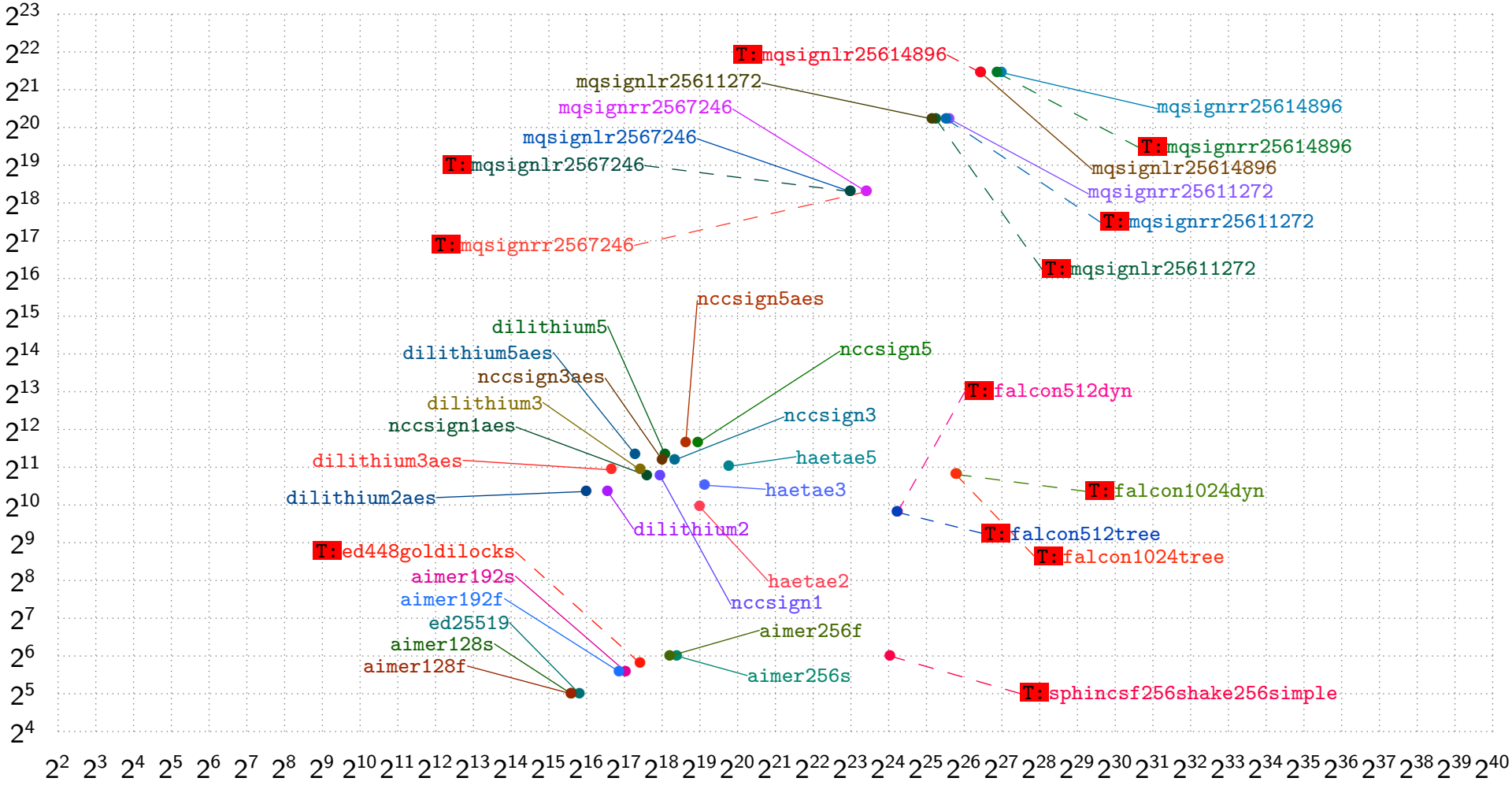


amd64, titan0, crypto_sign, keypair time, key size https://bench.cr.yp.to

Horizontal axis: Time (cycles) to generate a public key (crypto_sign_keypair). 20241021

Vertical axis: Space (bytes) for a public key (crypto_sign_PUBLICKEYBYTES).

"T:" means that the SUPERCOP database does not list constant time as a goal for this implementation.

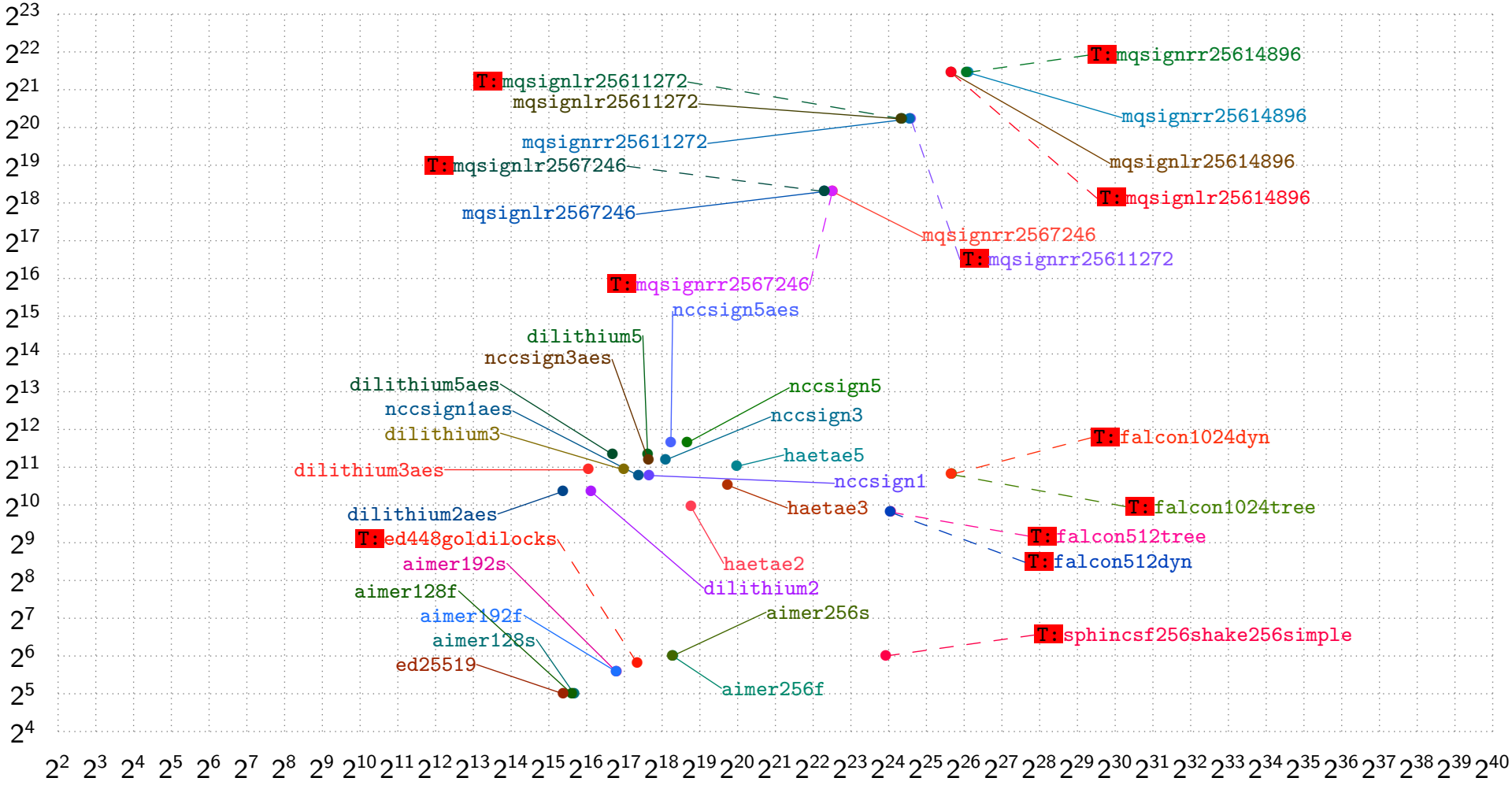


amd64, cezanne, crypto_sign, keypair time, key size https://bench.cr.yp.to

Horizontal axis: Time (cycles) to generate a public key (crypto_sign_keypair). 20241021

Vertical axis: Space (bytes) for a public key (crypto_sign_PUBLICKEYBYTES).

"T:" means that the SUPERCOP database does not list constant time as a goal for this implementation.

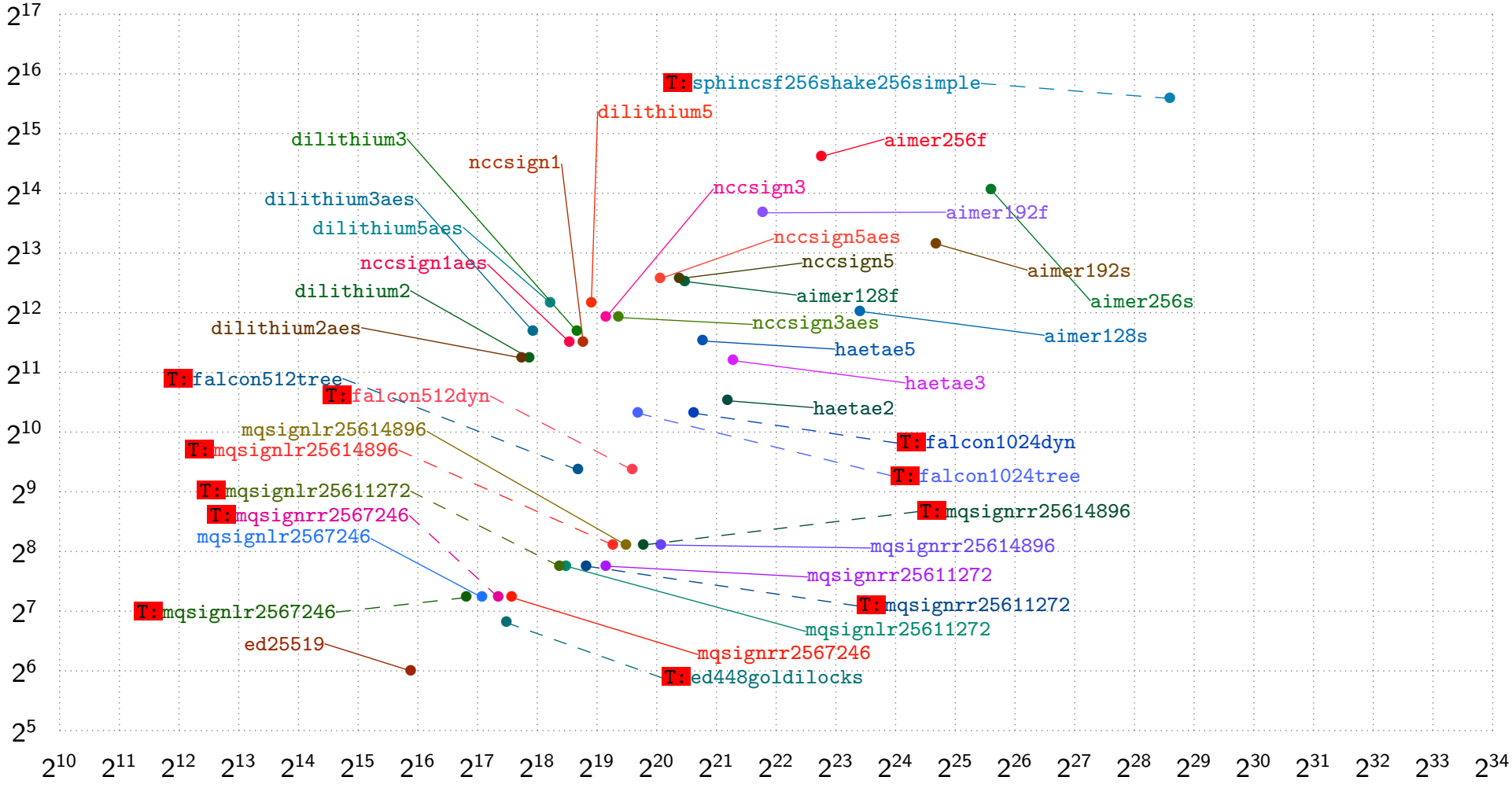


amd64, titan0, crypto_sign, sign time, signature size https://bench.cr.yp.to

Horizontal axis: Time (cycles) to generate a signed message given a message (crypto_sign). 20241021

Vertical axis: Space overhead (bytes) for signing a long message (at most crypto_sign_BYTES).

"T:" means that the SUPERCOP database does not list constant time as a goal for this implementation.

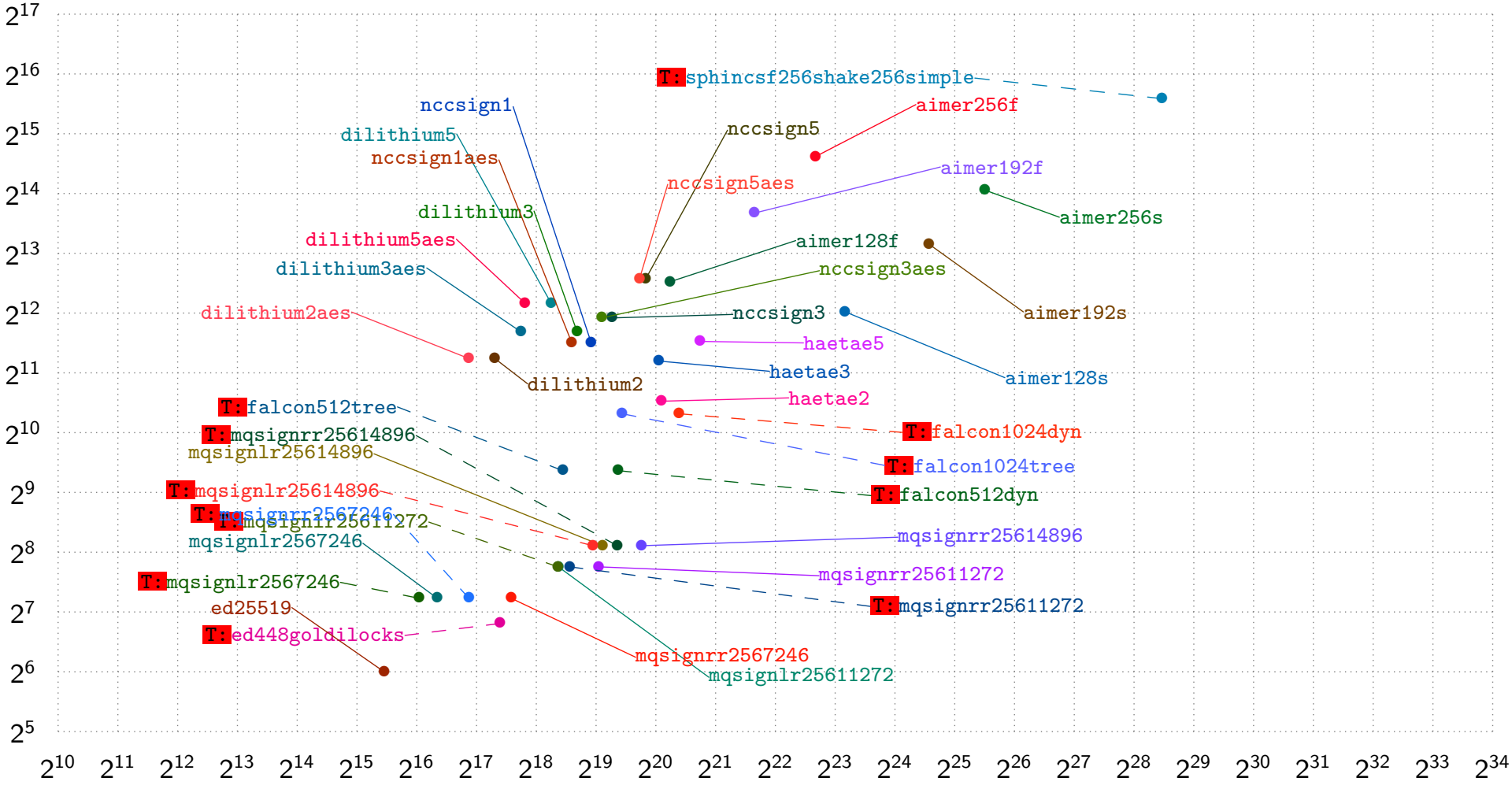


amd64, cezanne, crypto_sign, sign time, signature size https://bench.cr.yp.to

Horizontal axis: Time (cycles) to generate a signed message given a message (crypto_sign). 20241021

Vertical axis: Space overhead (bytes) for signing a long message (at most crypto_sign_BYTES).

"T:" means that the SUPERCOP database does not list constant time as a goal for this implementation.

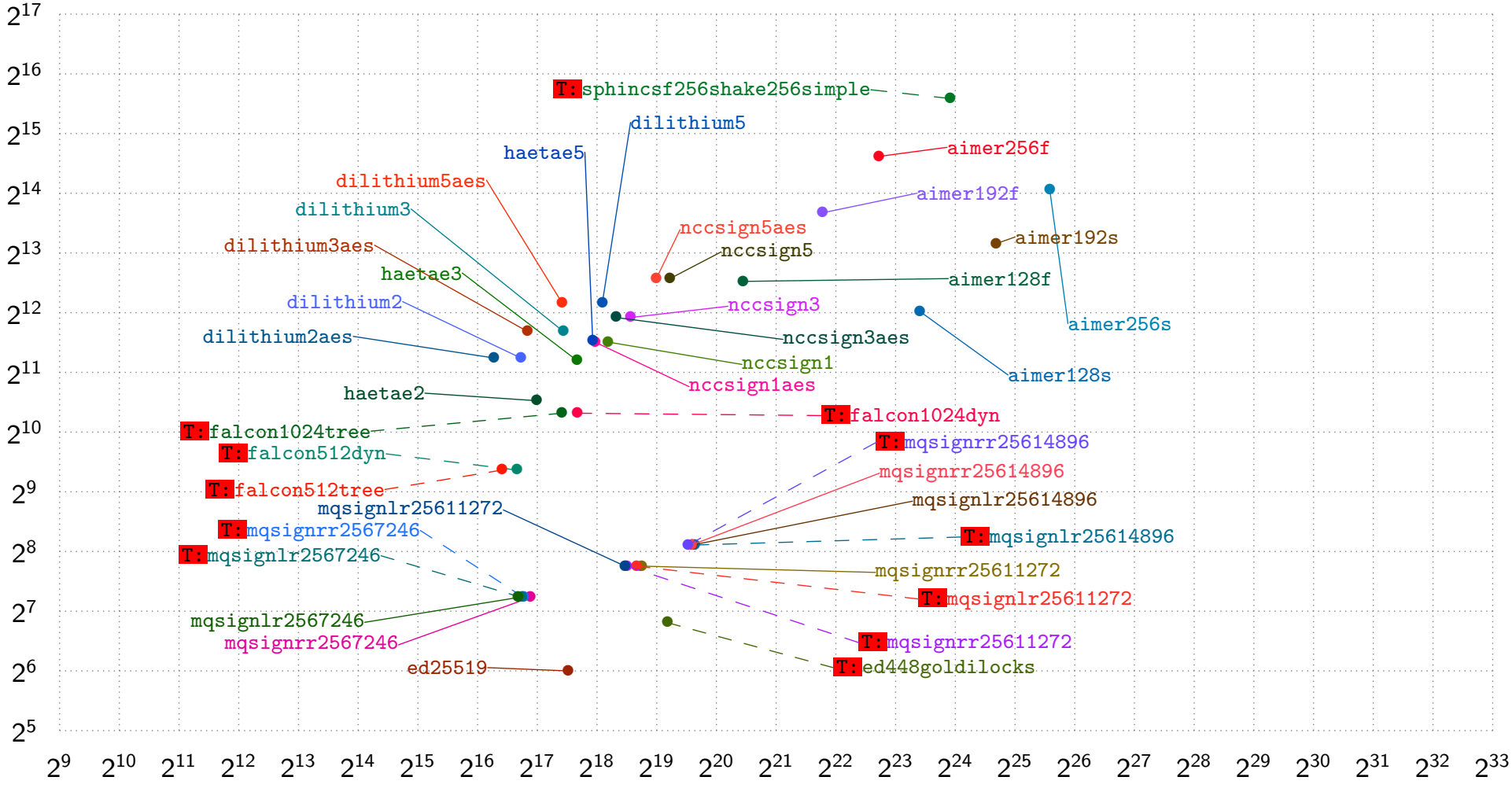


amd64, titan0, crypto_sign, open time, signature size https://bench.cr.yp.to

Horizontal axis: Time (cycles) to generate a message given a signed message (crypto_sign_open). 20241021

Vertical axis: Space overhead (bytes) for signing a long message (at most crypto_sign_BYTES).

"T:" means that the SUPERCOP database does not list constant time as a goal for this implementation.

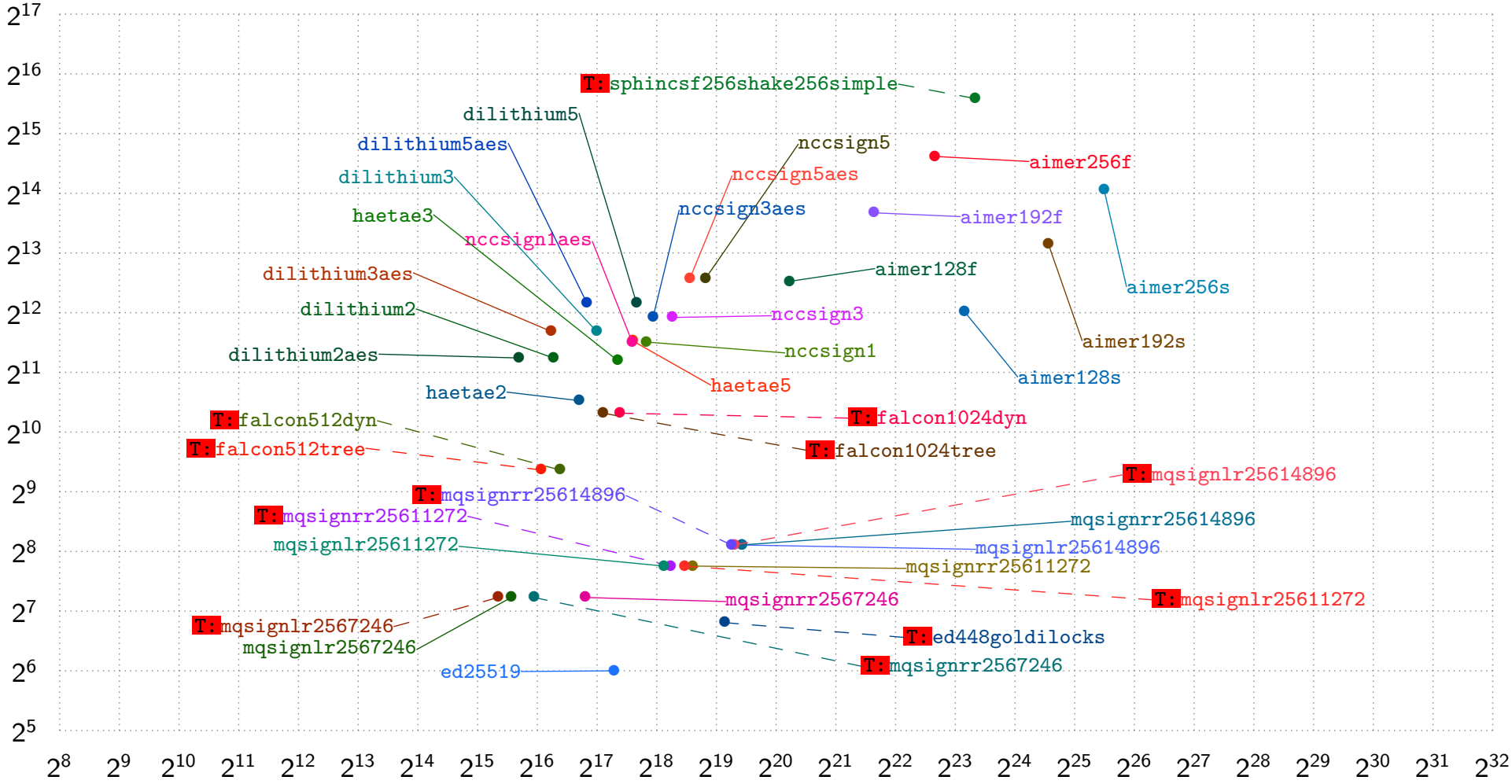


amd64, cezanne, crypto_sign, open time, signature size https://bench.cr.yp.to

Horizontal axis: Time (cycles) to generate a message given a signed message (crypto_sign_open). 20241021

Vertical axis: Space overhead (bytes) for signing a long message (at most crypto_sign_BYTES).

"T:" means that the SUPERCOP database does not list constant time as a goal for this implementation.

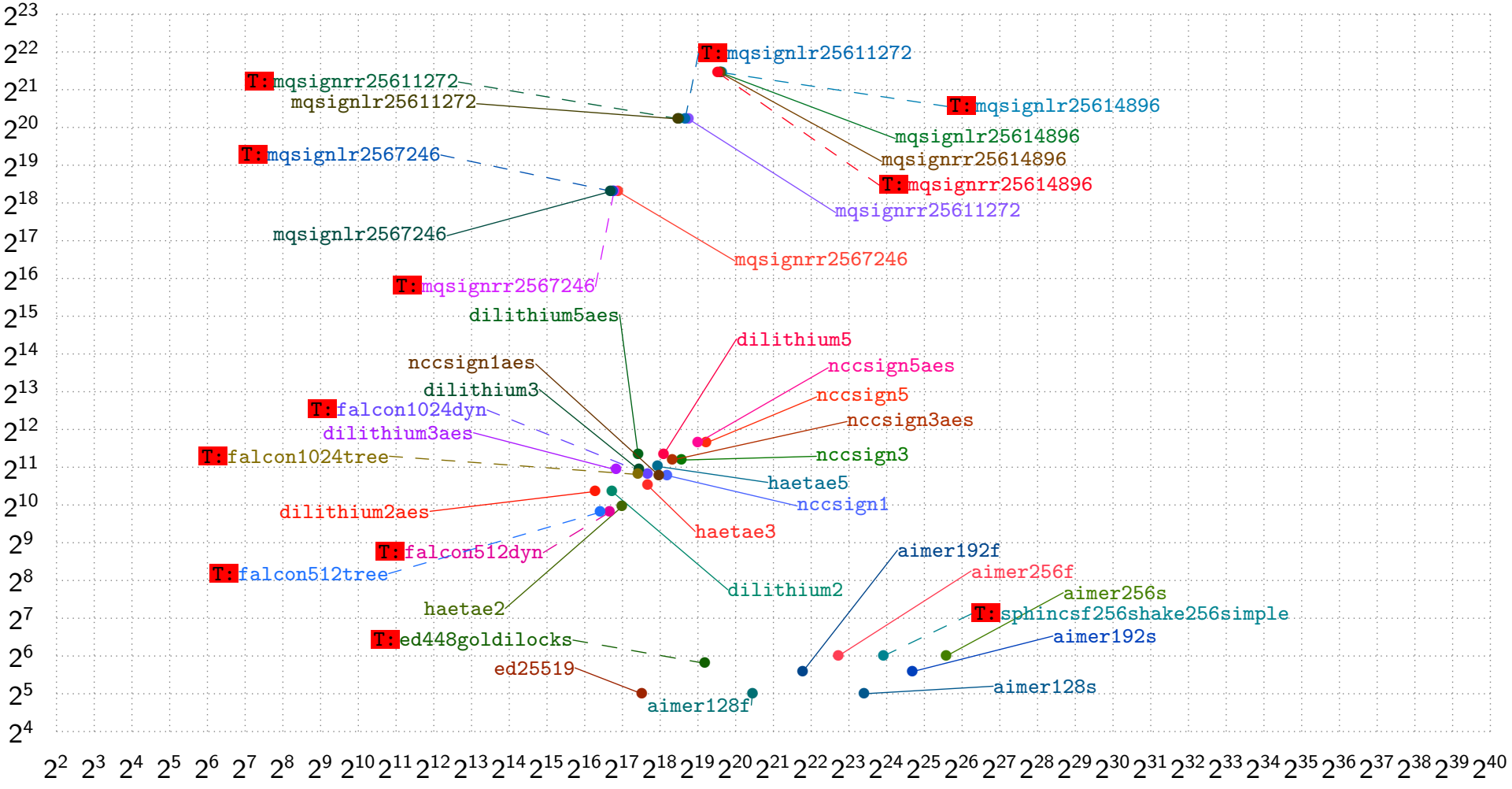


amd64, titan0, crypto_sign, open time, key size https://bench.cr.yp.to

Horizontal axis: Time (cycles) to generate a message given a signed message (crypto_sign_open). 20241021

Vertical axis: Space (bytes) for a public key (crypto_sign_PUBLICKEYBYTES).

"T:" means that the SUPERCOP database does not list constant time as a goal for this implementation.

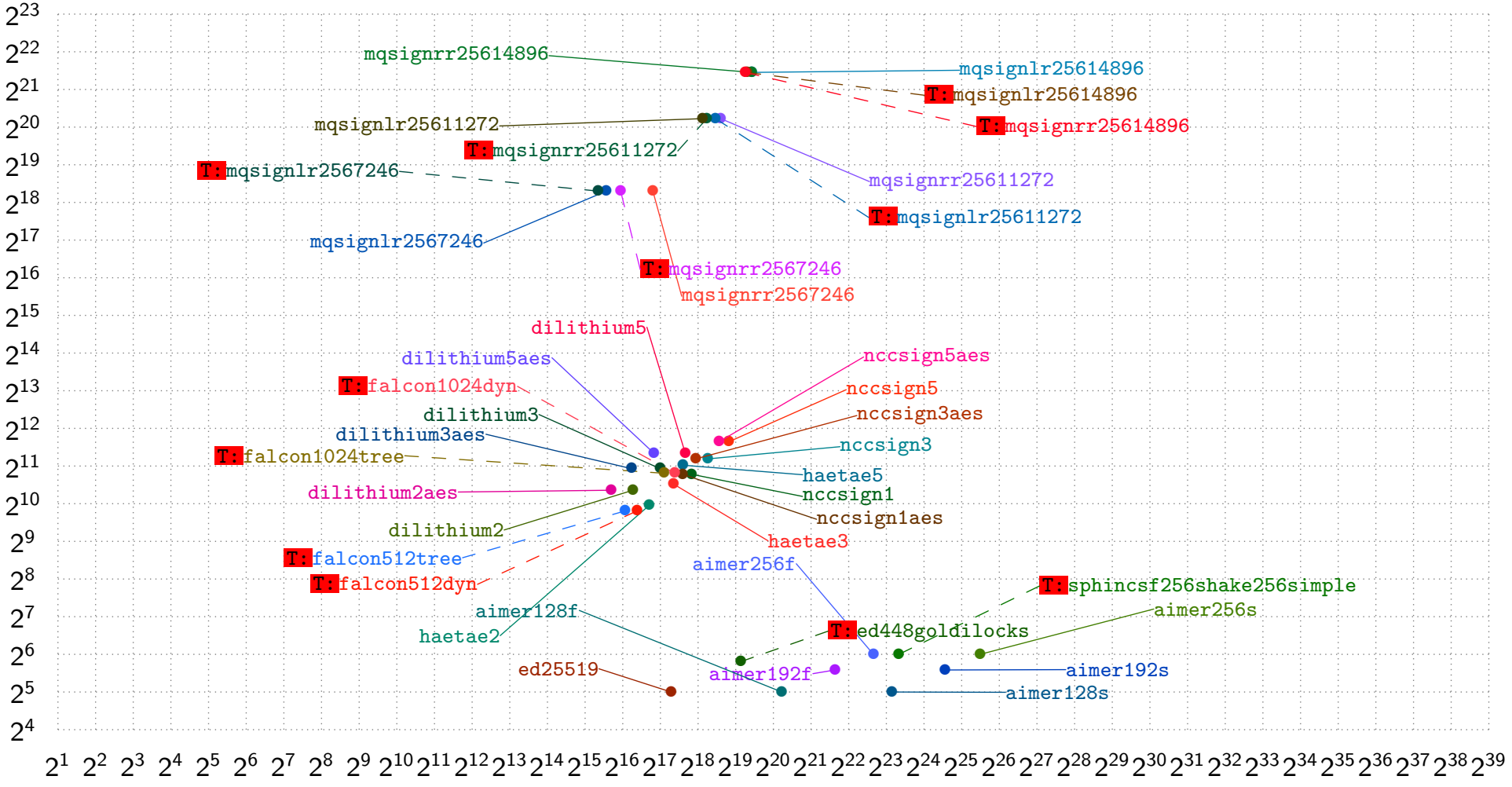


amd64, cezanne, crypto_sign, open time, key size https://bench.cr.yp.to

Horizontal axis: Time (cycles) to generate a message given a signed message (crypto_sign_open). 20241021

Vertical axis: Space (bytes) for a public key (crypto_sign_PUBLICKEYBYTES).

"T:" means that the SUPERCOP database does not list constant time as a goal for this implementation.



KEMs

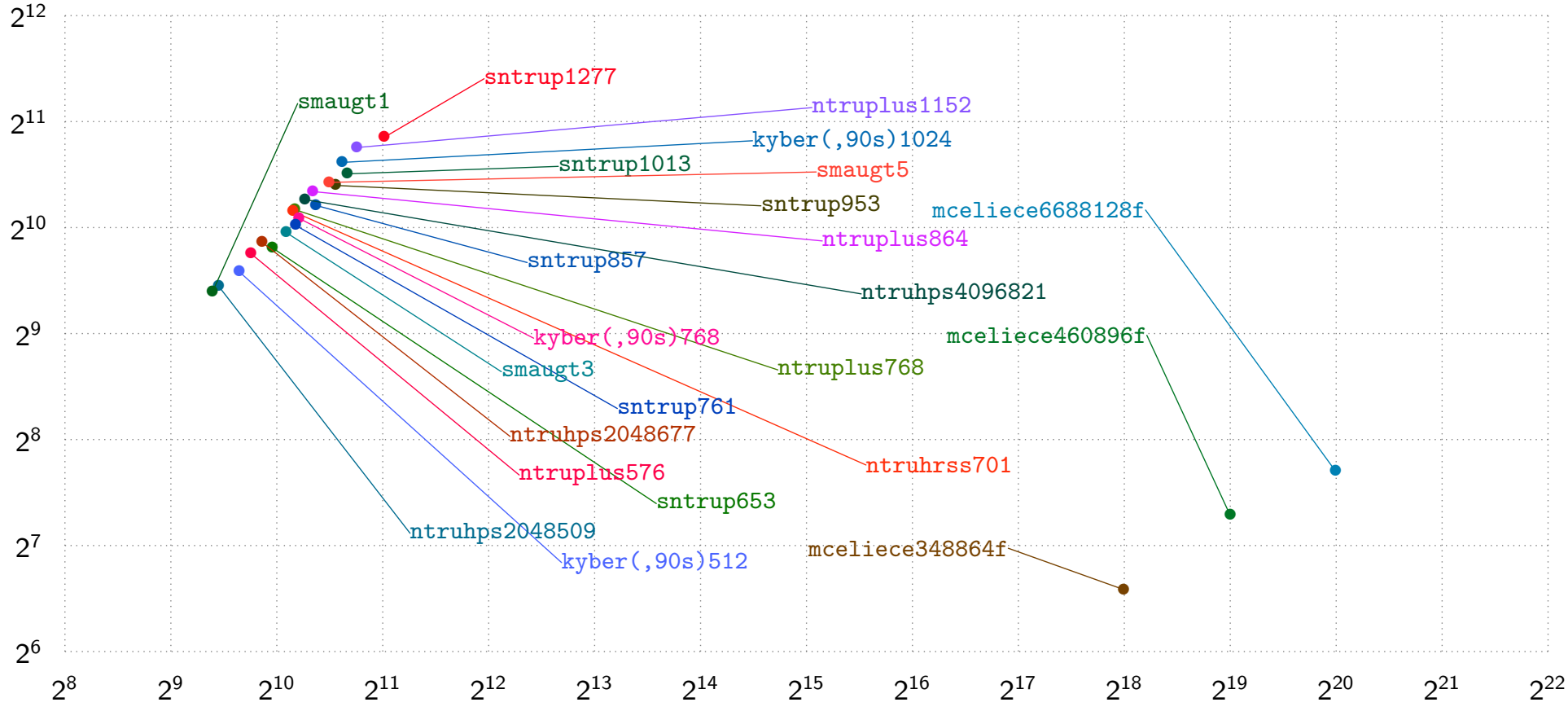
amd64, titan0, crypto_kem, key size, ciphertext size

https://bench.cr.yp.to

20241021

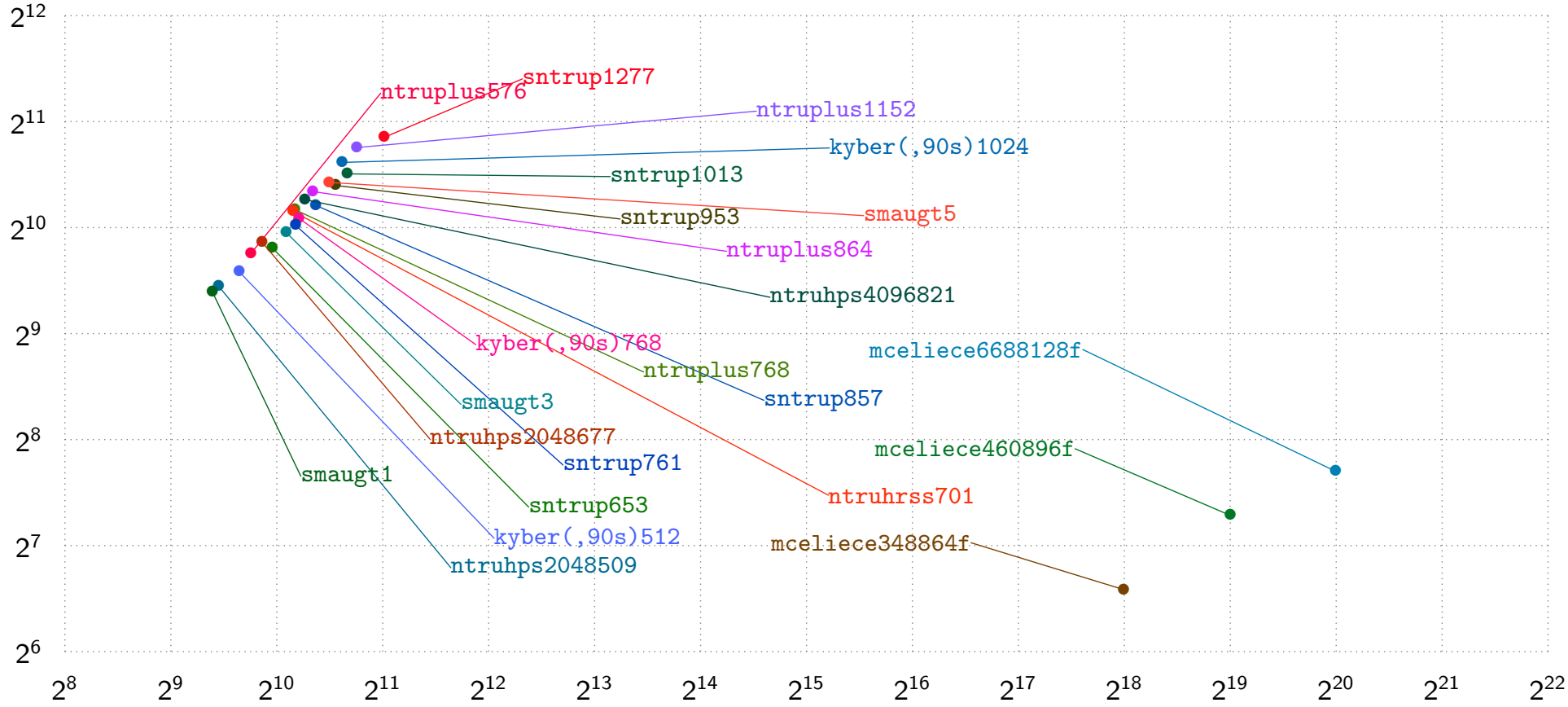
Horizontal axis: Space (bytes) for a public key (crypto_kem_PUBLICKEYBYTES).

Vertical axis: Space (bytes) for a ciphertext (crypto_kem_CIPHERTEXTBYTES).

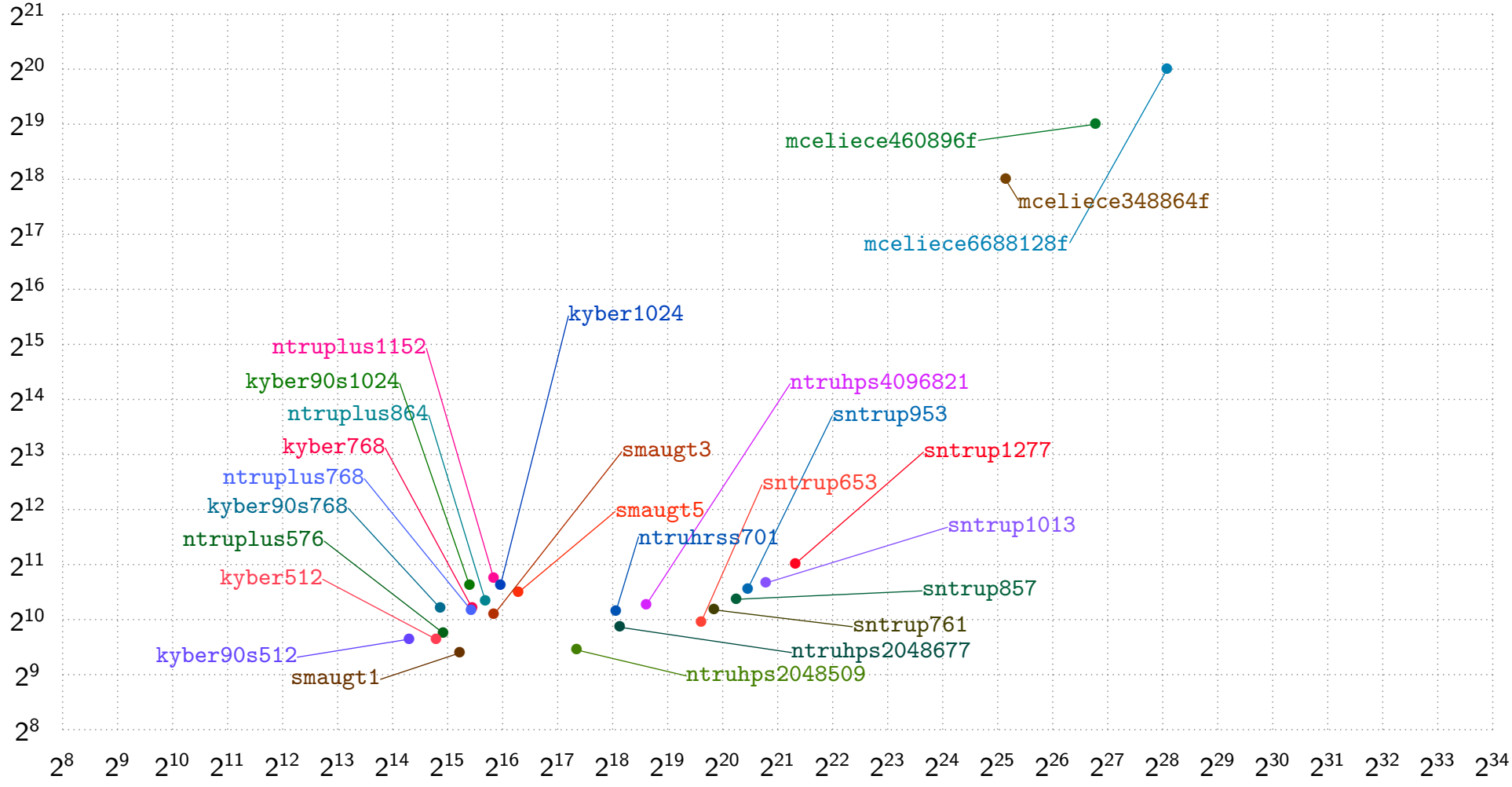


amd64, cezanne, crypto_kem, key size, ciphertext size
Horizontal axis: Space (bytes) for a public key (crypto_kem_PUBLICKEYBYTES).
Vertical axis: Space (bytes) for a ciphertext (crypto_kem_CIPHERTEXTBYTES).

https://bench.cr.yp.to
20241021



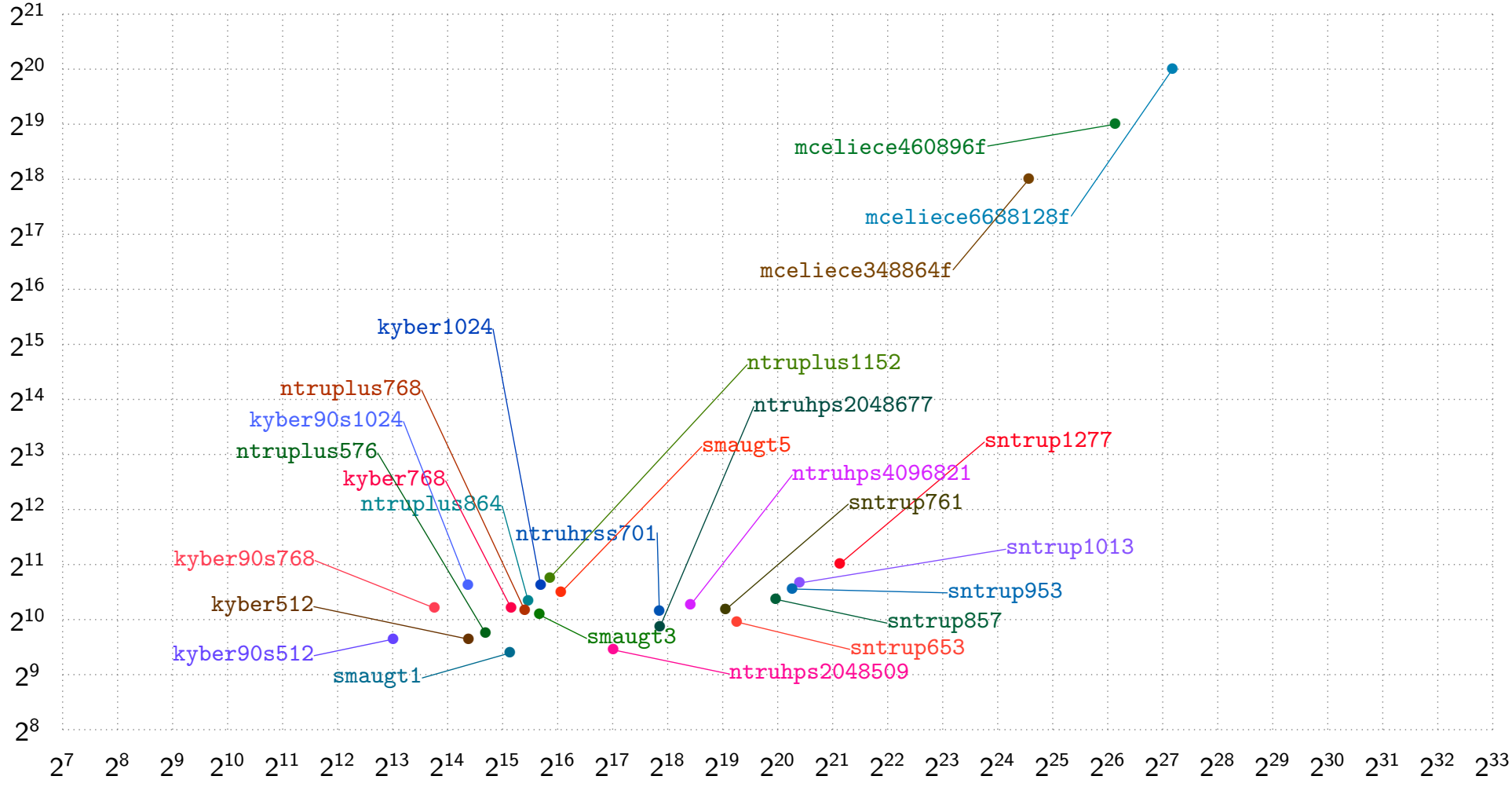
amd64, titan0, crypto_kem, keypair time, key size https://bench.cr.yp.to
Horizontal axis: Time (cycles) to generate a public key (crypto_kem_keypair). 20241021
Vertical axis: Space (bytes) for a public key (crypto_kem_PUBLICKEYBYTES).



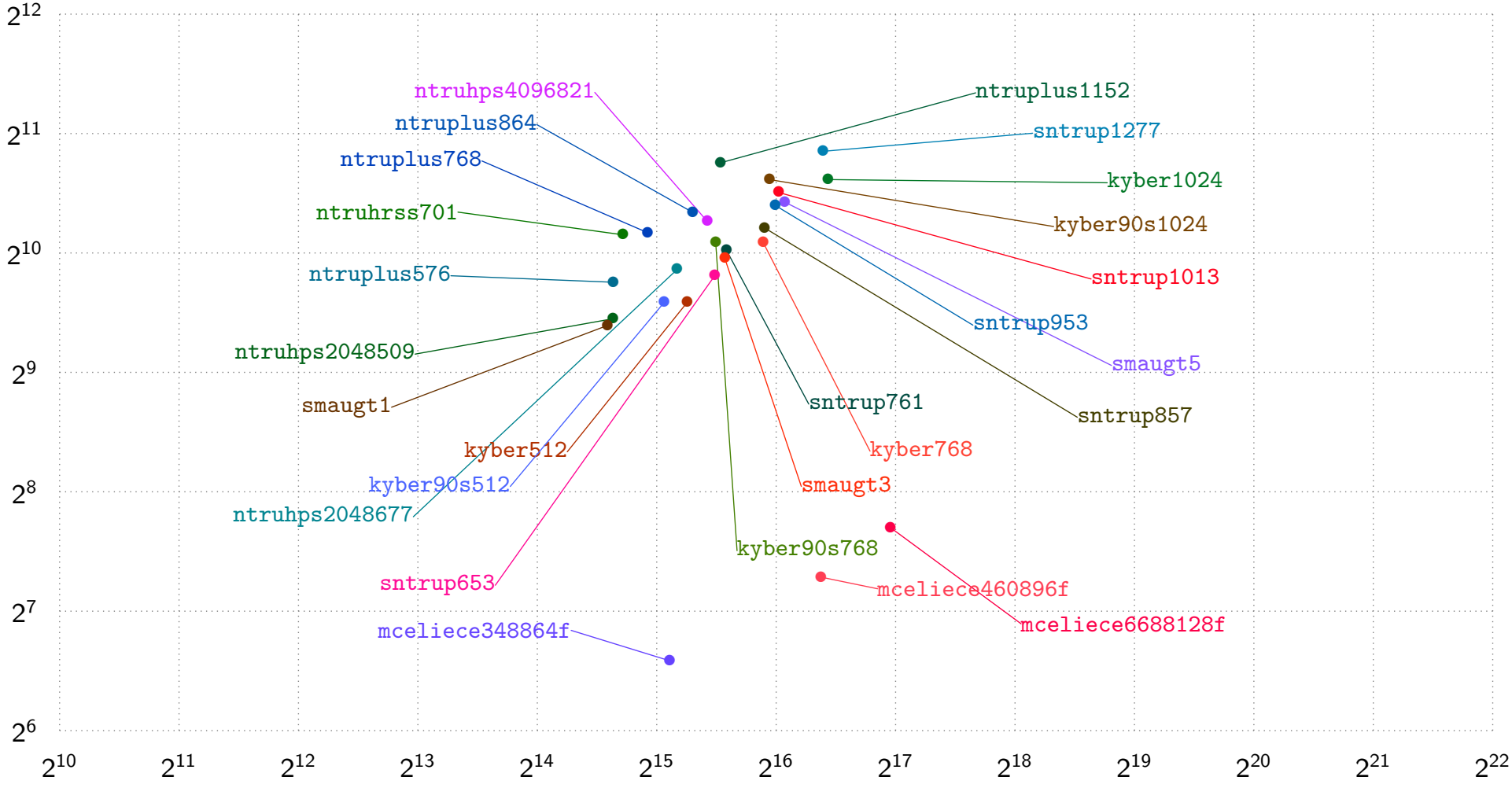
amd64, cezanne, crypto_kem, keypair time, key size https://bench.cr.yp.to

Horizontal axis: Time (cycles) to generate a public key (crypto_kem_keypair). 20241021

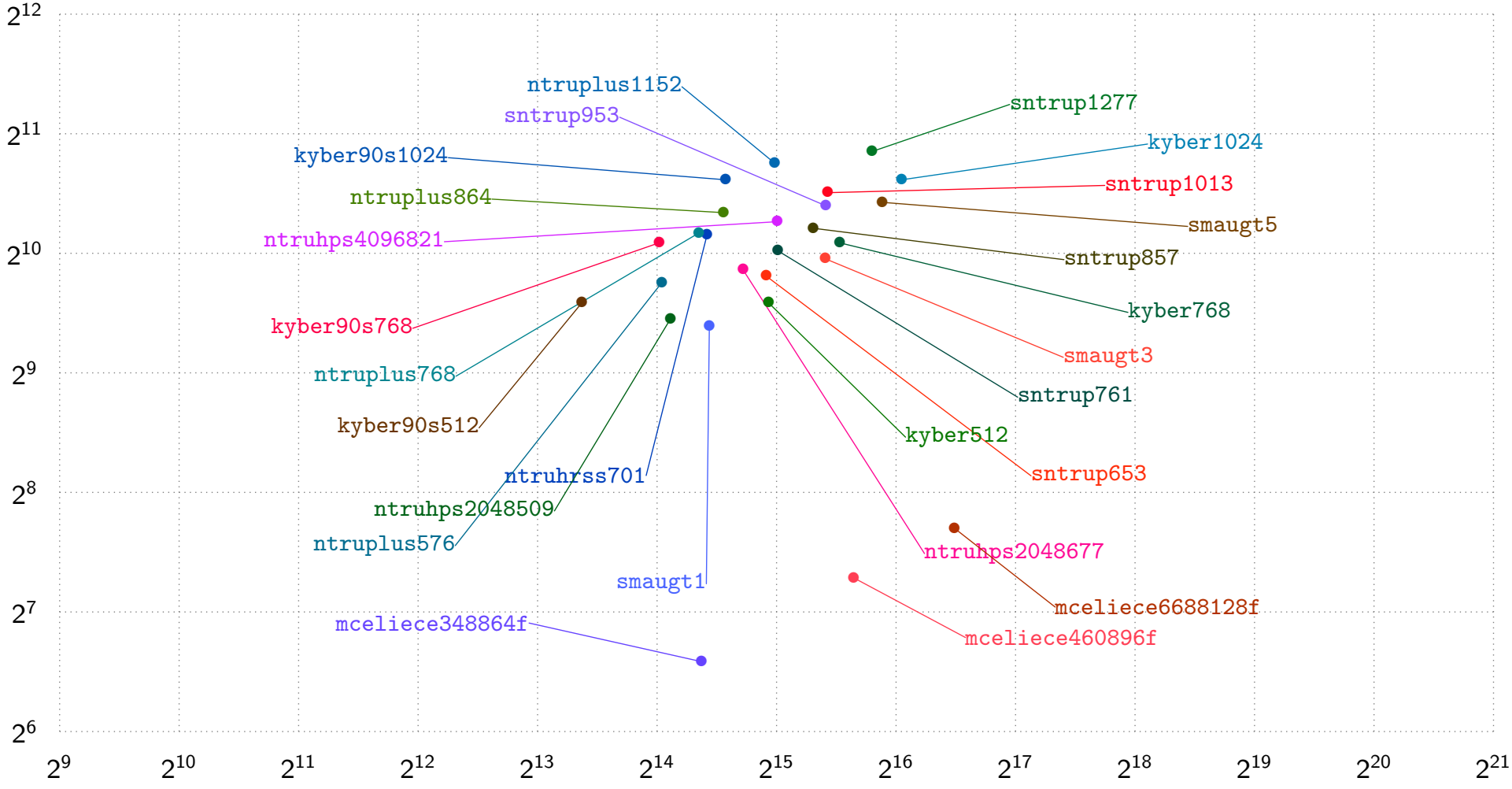
Vertical axis: Space (bytes) for a public key (crypto_kem_PUBLICKEYBYTES).



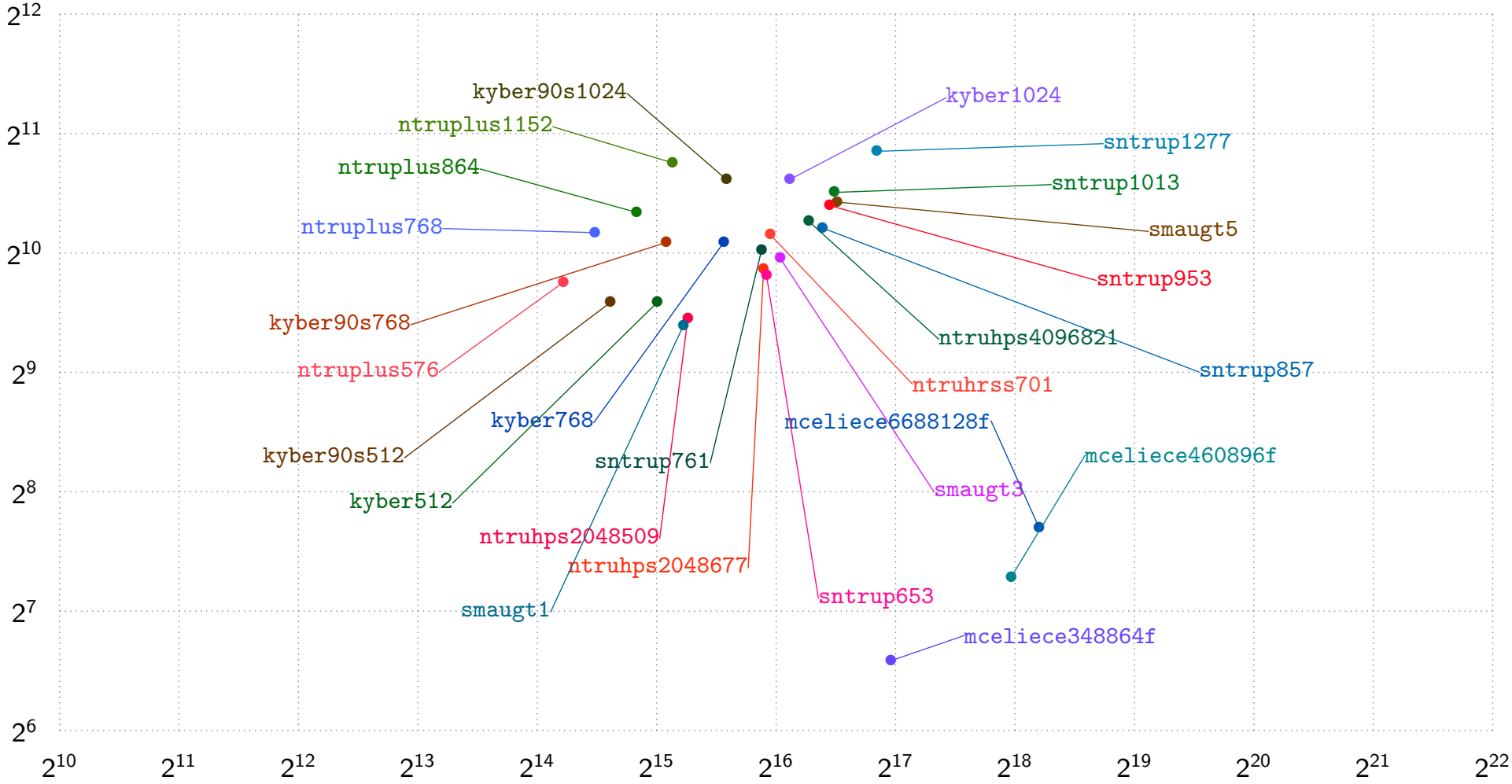
amd64, titan0, crypto_kem, enc time, ciphertext size https://bench.cr.yp.to
Horizontal axis: Time (cycles) to generate a ciphertext given a public key (crypto_kem_enc). 20241021
Vertical axis: Space (bytes) for a ciphertext (crypto_kem_CIPHERTEXTBYTES).



amd64, cezanne, crypto_kem, enc time, ciphertext size https://bench.cr.yp.to
Horizontal axis: Time (cycles) to generate a ciphertext given a public key (crypto_kem_enc). 20241021
Vertical axis: Space (bytes) for a ciphertext (crypto_kem_CIPHERTEXTBYTES).



amd64, titan0, crypto_kem, dec time, ciphertext size https://bench.cr.yp.to
Horizontal axis: Time (cycles) to generate a session key given a ciphertext (crypto_kem_dec). 20241021
Vertical axis: Space (bytes) for a ciphertext (crypto_kem_CIPHERTEXTBYTES).



amd64, cezanne, crypto_kem, dec time, ciphertext size https://bench.cr.yp.to
Horizontal axis: Time (cycles) to generate a session key given a ciphertext (crypto_kem_dec). 20241021
Vertical axis: Space (bytes) for a ciphertext (crypto_kem_CIPHERTEXTBYTES).