Hello Crystals team.

I was wondering if it’s possible to use smaller parameter sets to decrease the signature size, instead of relying on aggressive compression techniques used in the current form of Dilithium.

Specifically, if we were to preserve the \( \mathbb{Z}_q[X]/(X^{256}+1) \) module and matrix row and column counts in the current specification, and decrease ‘q’ and acceptance threshold of signature variable ‘z’, and avoid public-key compression, would we be able to achieve comparable bandwidth efficiency and security? Had the team done some calculation on this?

Thanks.