



LMS Parameter Sets

Scott Fluhrer
July 25, 2023

History of the LMS “more parameters” draft

The CFRG created RFC 8554, which defined LMS, a stateful hash based signature algorithm

Only parameter sets with SHA-256 were specified.

To expand these choices, Quynh Dang (NIST) and I created

`draft-fluhrer-lms-more-param-sets`

This draft defines parameter sets with the options:

- SHA-256/192 (SHA-256 truncated to 192 bits)
- SHAKE-256 (at 192 and 256 bits of output length)

Status of this draft

IANA has assigned code points for the new parameter sets

NIST Special Publication 800-208 includes references to these parameter sets

I believe that the only thing blocking it from being an RFC is additional review

