From: Kelsey, John M. (Fed)
To: internal-pqc
Subject: Strong binding
Date: Saturday, October 9, 2021 3:37:24 PM

Everyone,

Off the top of my head, wouldn't every scheme have strong binding except SPHINCS+? With SPHINCS+, the signer could find M, M' such that sign(PK,M) = sign(PK,M'), since the signer knows the prefix/randomization for the hash. And really, this is just a design decision—accepting that the signer could create such collisions lets you shrink the signatures by about a factor of two. Are there any other schemes that only sign (say) a 128-bit randomized hash for Level 1 security?

--John