From: Kerman, Sara J. (Fed)
To: Brown, Evelyn A (Fed)
Subject: CSD WERB Update
Date: Monday, December 12, 2016 1:10:00 PM

Evelyn,
The following pub went to ITL today for review:
NIST SP 800-185: SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash and ParallelHash (Pub # 922422)
Authors: Kelsey, John M. M. ; **Chang**, Shu-jen H. H. ; **Perlner**, Ray A. ;
Abstract: This Recommendation specifies four types of SHA-3-derived functions: cSHAKE, KMAC, TupleHash, and ParallelHash, each defined for a 128- and 256-bit security strength. cSHAKE is a customizable variant of the SHAKE function, as defined in FIPS 202. KMAC (for KECCAK Message Authentication Code) is a variable-length message authentication code algorithm based on KECCAK; it can also be
used as a pseudorandom function. TupleHash is a variable-length hash function designed to hash tuples of input strings without trivial collisions. ParallelHash is a variable-length hash function that can hash very long messages in parallel.
This paper also went to ITL today for review:
IACR ePrint/PKC 2017 Towards Tightly Secure Short Signatures and IBE, Revisited (PUB #922105)
Authors: Alperin-Sheriff, Jacob; Apon, Daniel
Abstract: The Boyen-Li signature scheme [Asiacrypt'16] is a major theoretical breakthrough. Via a clever homomorphic evaluation of a pseudorandom function over their verification key, they achieve a reduction loss in security linear in the underlying security parameter and entirely independent of the number of message queries made, while still maintaining short signatures (consisting of a single short lattice vector). All previous schemes with such an independent reduction loss in security required a linear number of such lattice vectors, and even in the classical world, the only schemes achieving short signatures relied on non-standard assumptions. Unfortunately, the scheme suffers from an infeasibly massive verification key and even more infeasibly slow signing and verification algorithms. In addition, it makes some questionable claims regarding quantum-safe security, and has a less-than-rigorous proof of security.
We improve on their result, providing a rigorous proof of security, a verification key smaller by a linear factor, a significantly tighter reduction with only a constant loss, and signing and verification algorithms that could plausibly run in about 1 second. Our main idea is to change the scheme in a manner that allows us to replace the pseudorandom function evaluation with an evaluation of a much more efficient weak pseudorandom function.
As a matter of independent interest, we give an improved method of randomized inversion of the G-gadget matrix [MP12], which reduces the noise growth rate in homomorphic evaluations performed in a large number of lattice-based cryptographic schemes, without incurring the high cost of sampling discrete Gaussians.

Sara J. Kerman
NIST
301-975-4634
sara@nist.gov